

AGENDA  
KANSAS RACING AND GAMING COMMISSION  
10:00 a.m., Friday, September 11, 2020

TELECONFERENCE  
PHONE NUMBER: 1-888-321-5815  
CONFERENCE ID: 7962575

A. CALL TO ORDER

B. APPROVAL OF AGENDA

C. APPROVAL OF MINUTES

1. [Minutes of August 14, 2020](#)

D. CONSENT AGENDA

*Items listed on the consent agenda are routine in nature. If requested by a commissioner, an item may be removed from the Consent Agenda and placed under Commission Items for further discussion and consideration.*

1. Approvals and revocations for certain lottery facility games and related components
  - a. [GLI Approval Letters August 2020](#)
2. Internal Control amendment approvals
  - a. [Boot Hill Casino internal control amendment approvals](#)
  - b. [Kansas Star Casino internal control amendment approvals](#)
3. [Internal Cybersecurity Policies Staff Memo](#)
  - a. [2020-01](#)
  - b. [2020-02](#)
  - c. [2020-04](#)
  - d. [2020-05](#)
  - e. [2020-06](#)
  - f. [2020-07](#)
  - g. [2020-08](#)
  - h. [2020-09](#)

- i. [2020-10](#)

E. LOTTERY GAMING FACILITY REPORTS/ITEMS

- 1. Boot Hill Casino and Resort
  - a. [August Monthly Report](#)
  - b. [August Revenue Report](#)
- 2. Kansas Star Casino
  - a. [August Monthly Report](#)
  - b. [August Revenue Report](#)
- 3. Hollywood Casino at Kansas Speedway
  - a. [August Monthly Report](#)
  - b. [August Revenue Report](#)
- 4. Kansas Crossing Casino
  - a. [August Monthly Report](#)
  - b. [August Revenue Report](#)

F. COMMISSION ITEMS – OLD BUSINESS

NONE

G. COMMISSION ITEMS – NEW BUSINESS

- 1. FY 2021 and 2022 Budget

<i>Commission Action</i>	<i>Commission review and discussion</i>
<i>Staff Presentation</i>	<i>Brandi White, Director of Administration, Finance, and Audit, KRGC Stephanie Nickoley, Director of Human Resources and Finance, State Gaming Agency</i>

*Staff Recommendation*      *Approval of the proposed Budget*

- a. [Kansas Racing and Gaming Commission FY 2021 and 2022 Budget Memo](#)
- b. [State Gaming Agency FY 2021 and 2022 Budget Memo](#)

## H. PUBLIC COMMENTS

## I. STAFF REPORTS

1. Sarah Lynch-Chaput, Paralegal
  - a. [Voluntary Exclusion Program Report](#)
2. Don Brownlee, Executive Director

## J. EXECUTIVE SESSIONS

*The Commission conducts executive sessions in accordance with the Kansas Open Meetings Act and all discussions are limited to the specified purposes listed in K.S.A. 75-4319. The Commission utilizes executive sessions to consult with the Commission's attorney on confidential legal matters, to discuss confidential personnel matters, to protect the confidentiality of necessarily closed information including licensee background reports, and to protect the integrity of gaming information and the confidentiality of lottery gaming facility manager finances. **Note: Due to logistical issues with convening a closed executive session mid-meeting and reconvening the meeting to take agency action, the closed executive session will take place immediately prior to the meeting. This procedure will be in place for commission meetings held during the COVID-19 closures and will be discontinued once the commission resumes in-person meetings. The following items will be discussed:***

1. Attorney/Client Privilege
2. Background Reports

## K. OTHER BUSINESS/FURTHER COMMISSION ACTION

1. Consideration of proposed gaming licenses and renewals

## L. ADJOURNMENT

## KANSAS RACING AND GAMING COMMISSION

### MINUTES – AUGUST 14, 2020

CALL TO ORDER  
(A.)

Chairman Brandon Jones called the August 14, 2020 meeting to order at 10:02 a.m. The meeting was held via teleconference. Notice of this teleconference was given to the public via the KRGC website, Public Square website, and social media. Commissioners David Moses, Kelly Kultala, Larry Turnquist, and Dave Myres were also present. Others present included Executive Director Don Brownlee, General Counsel Judith Taylor, Director of Administration, Audit, and Finance Brandi White, Director of Electronic Gaming Roger Bailey, Director of Security Joe Herridge, Recording Secretary Sarah Lynch-Chaput, and other staff.

MOTION, APPROVE  
AGENDA  
(B.)

Commissioner Moses (Myres) moved to approve the agenda. Motion carried unanimously.

MOTION, APPROVE  
JULY 17, 2020  
MEETING MINUTES  
(C.1.)

Commissioner Kultala (Turnquist) moved to approve the minutes of the July 17, 2020 meeting. Motion carried unanimously.

MOTION, APPROVE  
CONSENT AGENDA  
(D.)

Commissioner Myres (Kultala) moved to approve the consent agenda. Motion carried unanimously.

LOTTERY GAMING  
FACILITY  
REPORTS/ITEMS; BOOT  
HILL CASINO & RESORT  
(E.1.a.)

Diane Giardine, General Manager, reported:

- July 2020 revenue numbers compared to July 2019:
  - Total gaming revenue down 4.47%
  - Total slot revenue up 1.96%
  - Table games revenue down 41.85%
- Events and Promotions:
  - Earn & Eat Mondays
  - Weekly Food and Beverage Specials
  - Comp Point Multiplier Thursdays
  - Smash the Piggy Bank Fridays
  - \$100,000 Big Draw Saturdays
  - Bridal & Women's Day Out Expo, Sept. 13<sup>th</sup>
- Boot Hill Casino's COVID-19 precautions and the impact on staff and patrons

LOTTERY GAMING  
FACILITY  
REPORTS/ITEMS; KANSAS  
STAR  
(E.2.a.)

Jeff Babinski, Vice President and General Manager, reported:

- July 2020 revenue numbers compared to July 2019:
  - Admissions down 43.1%
  - Total gross gaming revenue down 14.4%
  - Slot coin-in down 13.6%
  - Slot hold up 0.15 points
  - Table games drop down 20.5%
  - Table games hold down 0.7 points
  - Poker room remains closed
- Events and Promotions:
  - Wichita Flea Market, July 25<sup>th</sup> and 26<sup>th</sup>
  - Wichita Flea Market, August 22<sup>nd</sup> and 23<sup>rd</sup>
  - Marauders Car Show, September 11<sup>th</sup> to 13<sup>th</sup>
- Kansas Star Casino's COVID-19 precautions and the impact on staff and patrons

LOTTERY GAMING  
FACILITY  
REPORTS/ITEMS;  
HOLLYWOOD CASINO AT  
KANSAS SPEEDWAY  
(E.3.a.)

Rick Skinner, Vice President and General Manager, reported:

- July 2020 revenue numbers compared to July 2019:
  - Total gaming revenue \$8.5 million, a decrease of 32.6%
  - Slot revenue \$8 million, a decrease of 29.3%
  - Table games revenue \$500,000, a decrease of 53%
  - Poker room remains closed
- Events and Promotions:
  - Ice Cream Maker Giveaway, July 31<sup>st</sup>
  - Sizzling Summer Free Bets - Table Games Promotion, Month of August
  - Free Pull & Get Full Promotion, August 8<sup>th</sup>
  - Kansas Lottery Scratch Ticket Giveaway, August 15<sup>th</sup>
  - VIP QuikTrip Gift Card Giveaway, August 22<sup>nd</sup>
  - Yeti Giveaway, August 28<sup>th</sup>
  - Gas Stove Giveaway, September 3<sup>rd</sup>
- Hollywood Casino's COVID-19 precautions and the impact on staff and patrons

LOTTERY GAMING  
FACILITY  
REPORTS/ITEMS; KANSAS  
CROSSING CASINO  
(E.4.a.)

Jeff McCain, General Manager, reported:

- July 2020 revenue numbers compared to July 2019:
  - Admissions down 29.2%
  - Net slot revenue up 0.8%

- Table games revenue down 47.7%
- Net gaming revenue down 3.9%
- Events and Promotions:
  - 8x Point Multipliers, August Tuesdays
  - Heat Wave Promotion, August Saturdays
  - Scratch Card Promotion, August Sundays
  - Casino Hot Seats, August 3<sup>rd</sup>, 13<sup>th</sup>, 17<sup>th</sup>, and 27<sup>th</sup>
  - Bank Account Bonanza Grand Prize Drawing, August 31<sup>st</sup>
- Kansas Crossing Casino's COVID-19 precautions and the impact on staff and patrons

COMMISSION ITEMS –  
OLD BUSINESS  
(F.)

There were no old business items.

COMMISSION ITEMS –  
NEW BUSINESS  
(G.)

There were no new business items.

PUBLIC COMMENTS  
(H.)

There were no public comments.

STAFF REPORTS  
(I.1.a. and I.2)

Sarah Lynch-Chaput, Paralegal, reported on the Voluntary Exclusion Program statistics for the month of July 2020.

Executive Director Brownlee reported:

- Kansas tribal casinos have all reopened.
- The Kansas Attorney General sued to set aside a court decision to allow the Wyandotte tribe of Oklahoma to open a casino on land in Park City, Kansas. The tribe's Chief has stated a casino will be opened on the property by the end of the year.
- The KRGC budget will be presented at the September commission meeting.
- The next meeting is scheduled for September 11, 2020 at 10:00 a.m.

EXECUTIVE SESSION;  
ATTORNEY-CLIENT  
PRIVILEGE AND  
BACKGROUND REPORTS  
(J.)

Due to the logistical issues of holding an executive session in the middle of the teleconference, the executive session was held immediately prior to the meeting. Prior notice of this change was given in the meeting agenda posted on the KRGC website and on the Public Square website. This procedure will only be used while the

commissioners and KRGC staff are working from home due to the COVID-19 pandemic. The executive session was held for the purpose of confidential attorney-client privileged communications and reviewing the list of confidential backgrounds for licensing. The commissioners, executive director and general counsel were included in the executive session portion for attorney-client privilege. The commissioners, executive director, general counsel and director of security were included in the executive session portion for reviewing the list of confidential backgrounds for licensing. No action was taken in executive session, and the subjects discussed were limited as previously described.

MOTIONS ON LICENSE  
APPLICATIONS  
(K.)

Commissioner Turnquist (Moses) moved to approve the 95 license applications from the August 14, 2020 list of background reports referred to the commission for action. Motion carried unanimously.

OTHER BUSINESS  
(L.)

No other business.

ADJOURN  
(M.)

The next meeting of the commission is on September 11, 2020 at 10:00 a.m. The meeting format will be decided and announced at a later time. Commissioner Kultala (Myres) moved to adjourn the meeting. Motion carried unanimously. The meeting was adjourned at 10:49 a.m.

SUBMITTED BY:

---

Larry Turnquist  
Secretary

APPROVED BY:

---

Brandon Jones  
Chairman

Manufacturer	File Number	Game Name
AINSWORTH GAMING TEC	MO-22-AWG-20-31	Lucky Empress
Aristocrat Technologies, Inc. *	MO-73-ARI-20-31	5.15.0-1.00.3
Aristocrat Technologies, Inc.	MO-73-ARI-20-39	Autumn Moon
Aristocrat Technologies, Inc.	MO-73-ARI-20-40	Autumn Moon
Aristocrat Technologies, Inc.	MO-73-ARI-20-41	Happy & Prosperous
Aristocrat Technologies, Inc.	MO-73-ARI-20-42	Panda Magic
Aristocrat Technologies, Inc.	MO-73-ARI-20-43	Golden Century
Aristocrat Technologies, Inc.	SY-73-ARI-20-13	N/A
Bally West	LO-00-SHU-19-25	I Luv Suits Poker Progressive
IGT	MO-22-IGT-18-12	OCEAN MAGIC GRAND
IGT	MO-22-IGT-18-127	GOLDEN JUNGLE GRAND
IGT	MO-22-IGT-18-71	GOLDEN EGYPT
IGT	MO-22-IGT-18-98	SCARAB
IGT	MO-22-IGT-20-65	Cobalt 23 meters
IGT	MO-59-IGT-19-08	Ocean Magic
IGT	MO-73-IGT-19-12	MAGIC OF THE NILE
IGT	MO-73-IGT-19-16	ZODIAC LION FREE GAMES
IGT	MO-73-IGT-20-58	UNIVERSAL ASCENT AND UC DIAGNOSTIC
IGT	SY-22-IGT-20-01	USB Downloadable UGAF0014
KONAMI GAMING INC.	MO-73-KON-19-103	KXP MBR
KONAMI GAMING INC.	MO-73-KON-19-110	KXP Run Time
KONAMI GAMING INC.	MO-73-KON-20-05	Windows 16GB MBR
KONAMI GAMING INC.	MO-73-KON-20-19	KPS - Silent Hill Premium Media Controller
KONAMI GAMING INC.	MO-73-KON-20-34	KXP Domestic Platform
KONAMI GAMING INC.	MO-73-KON-20-36	Silent Hill Escape
KONAMI GAMING INC.	MO-73-KON-20-37	Silent Hill Return
KONAMI GAMING INC.	MO-73-KON-20-46	Concerto Crescent & Stack (KXP) Conversion kit K-2837
KONAMI GAMING INC.	MO-73-KON-20-48	Concerto Opus/Dual (KXP) Conversion kit K-2838
KONAMI GAMING INC.	MO-73-KON-20-49	KX43 (KXP) Conversion kit K-2803
KONAMI GAMING INC.	MO-73-KON-20-55	Concerto Upright & Slant (KXP) Conversion Kit K-2861
KONAMI GAMING INC.	MO-73-KON-20-60	Piggy Pennies All Aboard
KONAMI GAMING INC.	MO-73-KON-20-64	Dynamite Dash All Aboard
KONAMI GAMING INC.	MO-73-KON-20-65	KXP Windows OS
KONAMI GAMING INC.	PA-73-KON-19-02	KX43 (KXP)
SDS	SY-509-SDS-20-02	CMP Tax Forms 13.x CMP Tax Forms 13.x EP2, CMP Tax Forms 13.x EP3
SG Gaming, Inc. f/k/a Bally Gaming, Inc.	MO-73-BAL-20-87	Money Link Maiden of the Hunt
SG Gaming, Inc. f/k/a Bally Gaming, Inc.	MO-99-BAL-20-02	Windows 5X
SG Gaming, Inc. f/k/a Bally Gaming, Inc.	MO-99-BAL-20-03	Operating System
* Executive Approval on 08/14/2020		

Eisenhower State Office Building  
700 SW Harrison, Suite 500  
Topeka, KS 66603



Phone: (785) 296-5800  
Fax: (785) 296-0900  
krgc@krgc.ks.gov  
krgc.ks.gov

Don Brownlee, Executive Director

Laura Kelly, Governor

### Boot Hill Casino Internal Control Amendments

September 11<sup>th</sup>, 2020

<b><u>Item #/ (Description)</u></b>	<b><u>Regulation Waiver?</u></b>	<b><u>Regulation/IC Reference</u></b>	<b><u>Staff Recommendation</u></b>
BH571 – EGM Off-Site Storage Key (WAIVER)	Yes	KAR 112-104-1(e) / IC140.070 ; IC 170.040	Approval
BH572 – Table Game Procedures	No	KAR 112-108-2, 108-4, 108-6, 108-7, 108-28, 108-36, 108-38, 108-55 / IC 200.002, .010, .020, .030, .080, .190, .210, .215	Approval

Eisenhower State Office Building  
700 SW Harrison, Suite 500  
Topeka, KS 66603



Phone: (785) 296-5800  
Fax: (785) 296-0900  
krgc@krgc.ks.gov  
krgc.ks.gov

Donald Brownlee, Executive Director

Laura Kelly., Governor

### Kansas Star Casino Internal Control Amendments

September 11, 2020

<b><u>Item #/ (Description)</u></b>	<b><u>Regulation Waiver?</u></b>	<b><u>Regulation/IC Reference</u></b>	<b><u>Staff Recommendation</u></b>
KS301 – Complimentaries	No	KAR 112-104-1, 112-104-9 / Administration Section 11 Complimentaries	Approve
KS302 – Security ICs & Plan	No	KAR 112-104-2 & 112-105-2 / Security Sections 2 & 3 & Security Plan	Approve
KS303 – Responsible Gambling Plan	No	KAR 112-112-3 / Responsible Gambling Plan	Approve



## STAFF AGENDA MEMORANDUM

**DATE OF MEETING:** September 11, 2020

**AGENDA ITEM:** Approval of specified agency cybersecurity policies

**PRESENTERS:** None – Consent Agenda

**ISSUE SUMMARY:** In 2018, the Kansas legislature passed the Kansas cybersecurity act, K.S.A. 75-7236 et seq. The act shifted cybersecurity responsibility from the Office of Information Technology Services (OITS) to the agency head. The agency head is now responsible for the security of all data (digital and physical) and information technology under that agency's purview. This responsibility extends to all locations of agency data, including remote sites, real property, data infrastructure, third party locations, and transmissions between locations. The Information Technology Executive Council (ITEC) determined the standards which the agency was required to follow, culminating in ITEC 7230A and ITEC 2400. The agency has drafted all applicable cybersecurity policies and is undergoing a phased review and approval process. The commission has received the following internal cybersecurity policies for review: 2019-01-01, 2019-01-02, 2019-01-04, 2019-01-05, 2019-01-06, 2019-01-07, 2019-01-08, 2019-01-09, and 2019-01-10. These policy names have been updated to: 2020-01, 2020-02, 2020-04, 2020-05, 2020-06, 2020-07, 2020-08, 2020-09, and 2020-10. Staff now requests formal approval.

**COMMISSION ACTION REQUIRED/REQUESTED:** Approve policies 2020-01, 2020-02, 2020-04, 2020-05, 2020-06, 2020-07, 2020-08, 2020-09, and 2020-10.

**STAFF RECOMMENDATIONS:** Staff recommends the commission approve the above-listed policies.

<b>Subject</b>		<b>Number</b>	<b>Draft #4</b>
<b>CYBERSECURITY POLICY INTRODUCTION &amp; TABLE OF CONTENT</b>		<b>2020-01</b>	
<b>Adopted</b> September 11, 2020	<b>Last Revision</b> March 13, 2020	<b>Rescinds</b>	
<b>Commission Authorization</b>			
Chairman Brandon Jones	Date		

## I. Purpose/Background

- A. The purpose of this policy is to fulfill the requirements of the Kansas Cybersecurity Act of 2018 by establishing eligibility for the assignment of agency-owned wireless communication devices, to establish policies for the use of such devices, to articulate the privacy expectations while using such devices, to assign responsibility for compliance with this policy, and to provide safety guidelines for the use of such equipment.
- B. The main purpose is to inform agency users (employees, contractors, and other authorized users) of their obligation to protect the technology and information assets of the agency. The Cybersecurity Policy describes the technology and information assets that must be protected and identifies many of the threats to those assets.

## II. Introduction

This Cybersecurity Policy is a formal set of rules with which those who are given access to agency technology and information assets must comply.

The Cybersecurity Policy describes a user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations, and informs users of the penalties for violations of the policy.

The Cybersecurity Policy also contains procedures for responding to incidents that threaten the security of agency computer systems and network.

## III. Identified Threats

- A. Employees

One of the biggest security threats is employees. Employees can cause damage to systems, either intentionally or through incompetence caused by a lack of judgment or training. Each employee is expected to know and comply with this Cybersecurity Policy. All KRGC staff are responsible for learning and remaining familiar with Data Management rules, Data Protection Requirements, and Minimum Security Standards in the Information Technology policies.

B. Amateur Hackers and Vandals

Except through spam and phishing, the probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. Attacks are typically well planned and are based on any weaknesses discovered that will allow a foothold into the network.

C. Professional Criminal Hackers and Saboteurs

The probability of this type of attack is low, but not completely unlikely, due to the amount of sensitive information contained in KRGC databases, or perceived connectivity to other databases.

D. Extreme Weather Conditions

The buildings housing the datacenters for KRGC are in a geographical area with weather conditions severe enough to possibly damage the datacenters in the event of a tornado, flooding, or high winds.

E. Power Outage

Power outage is a growing risk with aging power grids and the likelihood of severe weather. Power outages could affect KRGC components and/or third-party internet providers.

#### **IV. User Responsibilities and understandings**

A. Cybersecurity is not the sole responsibility of the KRGC IT/Cybersecurity departments. This policy establishes the usage policy for computer systems, networks, and information resources of the office. The policy applies to all employees and contractors who use the computer systems, networks, and information resources and to individuals who are granted access to the network for the agency's business purposes.

1. All users have a responsibility to immediately report any suspicious activity they observe in their email or in the system.

User accounts on agency computer systems are to be used only for business of the agency and not to be used for personal activities. Unauthorized use of the system

may be in violation of the law in addition to a violation of agency policy. Unauthorized use of the agency computing system and facilities may constitute grounds for either civil action or criminal prosecution.

2. Security is not an absolute.

KRGC can purchase the best security software, hire the best cybersecurity consultants, have the latest firewalls, but no system is completely invulnerable.

3. Communication between staff and IT is essential.

Staff members shall report possible threats for IT/Cybersecurity to address and should report work flow concerns, with the understanding that the needs of one do not always outweigh the needs of many. Security must ultimately outweigh convenience.

**V. Structure of policies**

A. For audit purposes and ease of tracking, the structure and order of these policies are similar to ITEC 7230A. All policies for Information Technology and Cybersecurity will be KRGC policies 2020-01. The numbering will mimic the sections in ITEC 7230A. The 7230A§ 8.0 mandates can be found in KRGC policy 2020-08. The 7230A§ 14.0 mandates can be found in KRGC policy 2020-14.

**B. TABLE OF CONTENTS**

KRGC Policy	Policy Title	ITEC 7230A Section	7230 Section Title
2020-01	Introduction & Table of Content	1.0	TITLE
2020-02	Newsletter	2.0	PURPOSE
2020-03	Vendor Affects	3.0	ORGANIZATIONS AFFECTED
2020-04	Intellectual Property	4.0	REFERENCES
2020-05	Definitions	5.0	DEFINITIONS
2020-06	Risk management & Data Classification	6.0	RISK MANAGEMENT STANDARD
2020-07	Assessment and security planning standard	7.0	ASSESSMENT AND SECURITY PLANNING STANDARD
2020-08	Awareness and training standard	8.0	AWARENESS AND TRAINING STANDARD
2020-09	Access control, Passwords, and Dual Authentication	9.0	ACCESS CONTROL

2020-10	Systems configuration	10.0	SYSTEMS CONFIGURATION STANDARD
2020-11	Data protection	11.0	DATA PROTECTION STANDARD
2020-12	Application processing	12.0	APPLICATION PROCESSING STANDARD
2020-13	Systems operations Data Protection & Patch priority	13.0	SYSTEMS OPERATIONS STANDARD
2020-14	Access to Individual User Electronic Information & Audits	14.0	SYSTEM AUDIT
2020-15	C-SIRT standard	15.0	INCIDENT RESPONSE STANDARD
2020-16	Physical security	16.0	PHYSICAL SECURITY
2020-17	Personnel security Cybersecurity Minimum Security Standards	17.0	PERSONNEL SECURITY
2020-18	IT purchasing and acquisition	18.0	SECURE PURCHASING/ACQUISITION STANDARD
2020-19	Initiation of Cybersecurity Policies	19.0	RESPONSIBILITIES
2020-20	KCJIS Policies	N/A	N/A
2020-21	Tabletop procedures, Waivers & Exceptions	N/A	N/A
2020-22	Disaster Recovery Plan	N/A	N/A
2020-23	Business Continuity Plan	N/A	N/A
2020-24	Password Security	N/A	N/A
2020-25	VPN policies and procedures	N/A	N/A
2020-26	Board of Trustees And Duties	NA	NA

APPENDIX A  
COPY OF ITEC 7230A

**Kansas Information Technology Executive Council**

- 1.0 TITLE: INFORMATION TECHNOLOGY SECURITY STANDARDS 7230A**
- 1.1 EFFECTIVE DATE: 07/1/2019
  - 1.2 TYPE OF ACTION: Update
  - 1.3 KEYWORDS: Kansas Information Technology Security Council, Enterprise Security Policy, Information Security, User Security, Personally Identifiable Information, Security Incident Response.
- 2.0 PURPOSE:** To define the Information Technology Policy 7230 minimum security standards and procedures for state of Kansas information systems.
- 3.0 ORGANIZATIONS AFFECTED:** All State of Kansas branches, boards, commissions, departments, divisions, agencies, and third parties used to process transmit or provide business capabilities on behalf of Kansas state government, hereafter referred to as Entity or Entities.
- 4.0 REFERENCES:**
- 4.1 K.S.A. 2013 Supp. 75-7203 authorizes the Kansas Information Technology Executive Council (ITEC) to: Adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state entities.
  - 4.2 Kansas Information Technology Executive Council (ITEC), ITEC Policy 7300, Revision 1, Information Technology Security Council Charter.
  - 4.3 Kansas Information Technology Executive Council (ITEC), ITEC Policy 7230, Revision 2, General Information Technology Enterprise Security Policy.
  - 4.4 NIST Special Publication 800-53 Rev 4 (latest version takes precedence) – Security and Privacy Controls for (Federal) Information Systems and Organizations.
  - 4.5 NIST Special Publication 800-88 Rev 1 (latest version takes precedence) – Guidelines for Media Sanitization.
  - 4.6 Federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 – Data security requirements for covered entities and their business associates.
- 5.0 DEFINITIONS:** The following definitions are applied throughout this document.
- 5.1 Critical System: Any Information System for which the loss, misuse, disclosure, unauthorized access to, or modification of information would result in a significant negative impact of an entity's core mission.
  - 5.2 Information Asset: A body of information defined and managed as a single unit, so it can be understood, shared, protected and exploited effectively.
  - 5.3 Information System: A discrete set of Information System Components organized

for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. Information Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

- 5.4 Information System Component: A discrete, identifiable information technology asset such as hardware, software, firmware, or media (electronic and hardcopy) that represents a building block of an Information System. Information System Components include commercial information technology products.
- 5.5 Multi-Factor Authentication (MFA): A method of confirming a User's claimed identity in which access is granted only after successfully presenting two or more different pieces of evidence (factors) to an authentication mechanism. Factors include knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).
- 5.6 Password: A memorized secret consisting of a sequence of words, special characters, or other text used to authenticate a User's identity.
- 5.7 Personal Financial Information (PFI): Any non-public personally identifiable financial information that an entity collects about an individual in order to provide a financial product or service.
- 5.8 Personally Identifiable Information (PII): Any information that can be used on its own or with other information to identify or locate a single person.
- 5.9 Portable Electronic Devices and Portable Electronic Media: Any electronic device or electronic media designed for easy transport. Examples of these items include but are not limited to: smart phones, tablets, laptops, USB flash media, SD cards, diskettes, CDs, DVDs, external hard drives, etc.
- 5.10 Production Information System: An Information System used to deliver essential services in the normal operating state of the entity.
- 5.11 Protected Health Information (PHI): Any information, in any form or medium, held or transmitted, about health status, provision of health care, or payment for health care that is created or collected by a covered entity or the business associates of a covered identity and can be linked to a specific individual. (Also see 45 CFR 160.103 – Code of Federal Regulations TITLE 45 – Public Welfare Part 160.103 Definitions).
- 5.12 Remote Access: Any access to an agency Information System by a User communicating through an external network (i.e. internet).
- 5.13 Restricted-Use Information (RUI): Includes PFI, PII, and PHI as defined in this Standard, as well as other regulated data (e.g. tax or criminal justice information) or information agencies designate as Restricted-Use Information due to their confidential or sensitive nature (e.g. physical or logical security information for state agencies and their systems).
- 5.14 Source Record: The authoritative instance of a record within an entity.
- 5.15 System Service Account: A special user account that an application or service uses to interact with an Information System.
- 5.16 User: Includes employees, contractors, or other agents acting on behalf of the state or carrying out state agency functions.
- 5.17 Variance or Exception: A deviation from a control mandated in this document.

## **6.0 RISK MANAGEMENT STANDARD**

- 6.1 Entities must develop a hierarchical Information Asset classification standard that assigns appropriate controls to each Information Asset classification. The standard must require that the security controls specified in this document be applied to Restricted-Use Information.
- 6.2 Entities must also set a default information classification for all information. If no default standard is created, all information must be considered Restricted-Use Information.
- 6.3 Entities must ensure that Information Asset trustees are appointed for the following Information Assets:
  - 6.3.1 Intellectual property or
  - 6.3.2 Data compilations that contain or may be projected to contain Source Records on thirty (30) or more individuals of Restricted-Use Information.
- 6.4 Information Asset trustees must perform the following tasks for each Information Asset:
  - 6.4.1 Determine the potential impact to the affected entity, individuals, and the State in the event of a loss of confidentiality, integrity, and availability of the Information Asset.
  - 6.4.2 Classify the asset in accordance with the entity's Information Asset classification standard.
  - 6.4.3 Ensure that the asset is handled in accordance with the entity's Information Asset handling standard.
  - 6.4.4 Ensure that adverse events are reported to the entity's Information Security Officer (ISO).
  - 6.4.5 Appoint Information Asset custodians.
  - 6.4.6 Approve all access and use of the Information Asset.
  - 6.4.7 Recertify annually the classification, access, users, and custodians of the Information Asset.
- 6.5 Information Asset custodians must perform the following responsibilities:
  - 6.5.1 Implement and operate the safeguards and controls for Information Assets as directed by Information Asset trustees.
- 6.6 Entities must implement a documented risk management process that addresses risk identification, tracking, mitigation, reporting, and acceptance.
- 6.7 Entities must document and track all outstanding risks (i.e. risk register).
- 6.8 Entities must periodically review existing risks.
- 6.9 Entities must process and approve any Variances or Exceptions to the requirements in this policy.
- 6.10 Entities must document, track, and report any approved Variances or Exceptions.

## **7.0 ASSESSMENT AND SECURITY PLANNING STANDARD RISK ASSESSMENT**

- 7.1 Entities must assess and document the risks to Information Systems that process, store or transmit Restricted-Use Information.
- 7.2 Entity risk assessments must identify potential threats and characterize the likelihood and impact of the threat being realized.
- 7.3 Entities must assess and document risks prior to placing an Information System into service, whenever a significant change is made, and at least once every three

(3) years thereafter.

## **SECURITY PLANNING**

- 7.4 Entities must document a security plan that specifies security controls based upon a risk assessment for Information Systems that process, store or transmit Restricted-Use Information.
- 7.5 The set of security controls in the security plan must be sufficient to adequately mitigate risks to organizational operations and assets, individuals, other organizations and the state, based on the entity risk tolerance.

## **8.0 AWARENESS AND TRAINING STANDARD - SECURITY AWARENESS TRAINING**

- 8.1 Entities must provide and conduct security awareness training for all Users.
- 8.2 Entities must require all Users to complete security awareness training within ninety (90) days of hire or initial access, and on an annual basis thereafter.
- 8.3 Entities must retain a form of acknowledgement of training completion.
- 8.4 Entities must review their security awareness training materials at least annually or more frequently as needed.
- 8.5 Awareness training must address the following topics at a minimum:
  - 8.5.1 Passwords including creation, changing, aging, and confidentiality
  - 8.5.2 Privacy and proper handling of sensitive information
  - 8.5.3 Physical security
  - 8.5.4 Social engineering
  - 8.5.5 Identity theft avoidance and action
  - 8.5.6 Email usage
  - 8.5.7 Internet usage
  - 8.5.8 Viruses and malware
  - 8.5.9 Software usage, copyrights, and file sharing
  - 8.5.10 Portable Electronic Devices and Portable Electronic Media
  - 8.5.11 Proper use of encryption devices
  - 8.5.12 Reporting of suspicious activity and abuse

## **9.0 ACCESS CONTROL - IDENTIFICATION AND AUTHENTICATION**

- 9.1 User access to Critical Systems or Information Systems that process, store or transmit Restricted-Use Information must be authorized by an appropriate Entity official through established protocols within the entity.
- 9.2 Users of Critical Systems or Information Systems that process, store or transmit Restricted-Use Information must be authenticated by a unique system identifier.
- 9.3 Users with administrative rights or elevated privileges must use a separate account to perform tasks that require elevated privileges or administrative rights.
  - 9.3.1 Administrative rights and elevated privilege accounts must only be used for activities that require elevated privileges (i.e. not for email access or internet browsing).
  - 9.3.2 Multi-Factor Authentication must be used for administrative rights or elevated privilege accounts.
  - 9.3.3 User accounts with administrative rights or elevated privileges must not

- have an email account or mailbox provisioned or associated with it.
- 9.4 System Service Accounts must be approved and documented for proper business use prior to creation and must be reviewed and approved annually for continued use.
  - 9.5 System Service Accounts must be configured with least privilege and only used for a single task or service.
  - 9.6 Unique system identifiers will be associated with a unique Information System authenticator (i.e. password, token, etc.).
  - 9.7 Unique Information System authenticators must be delivered in a secure and confidential manner.
  - 9.8 Passwords must not be viewable in clear text except by the account holder.
  - 9.9 Passwords must not be transmitted or electronically stored in clear text.
  - 9.10 Passwords must not be shared and must be kept confidential.
  - 9.11 Passwords for system User accounts must be constructed with the following requirements:
    - 9.11.1 A minimum of twelve (12) characters in length.
    - 9.11.2 Contain three (3) of four (4) of the following categories:
      - Uppercase
      - Lowercase
      - Numeral
      - Non-alpha numeric character
    - 9.11.3 Must not contain the user ID.
    - 9.11.4 Must not be changed more frequently than once every one (1) day without system administrator intervention.
    - 9.11.5 Must not have a lifespan that exceeds one hundred eighty (180) days.
    - 9.11.6 Must be different from the previous twenty-four (24) Passwords.
  - 9.12 Passwords for System Service Accounts must be constructed with the following requirements:
    - 9.12.1 A minimum of twelve (12) characters in length.
    - 9.12.2 Contain three (3) of four (4) of the following categories:
      - Uppercase
      - Lowercase
      - Numeral
      - Non-alpha numeric character
    - 9.12.3 Must not contain the user ID.
    - 9.12.4 Must not have a lifespan that exceeds three hundred sixty-five (365) days.
  - 9.13 Where tokens, whether soft tokens or physical tokens, as authenticators are used:
    - 9.13.1 A documented process must be followed for token distribution.
    - 9.13.2 A documented process must be followed for token revocation.
    - 9.13.3 A documented process must be followed for the handling of lost, stolen or damaged tokens.
  - 9.14 Where biometric data is used for authentication:
    - 9.14.1 A documented process must be followed for capturing user biometric data.
    - 9.14.2 A documented process must be followed for biometric revocation.
    - 9.14.3 A documented process must be followed for the handling of user biometric data.

## **ACCOUNT MANAGEMENT**

- 9.15 All Information System accounts must be configured according to the principle of least privilege.
- 9.16 Separation of duties must be enforced through account privileges.
  - 9.16.1 No single user account can have privileges to authorize, perform, review, and audit a single transaction.
  - 9.16.2 When available, role-based access controls (RBAC) must be implemented and enforced for systems that contain Restricted-Use Information or systems designated as a Critical System.
- 9.17 Information System accounts must be restricted to a maximum of five (5) consecutive failed attempts before being locked.
- 9.18 Accounts must remain locked for a minimum of thirty (30) minutes without administrator intervention.

## **SESSION MANAGEMENT**

- 9.19 Information Systems must display a system use notification identifying system ownership, system usage restrictions, prohibition of unauthorized access, implied consent and associated penalties for unauthorized access. The user must acknowledge the system use notification before gaining access to the Information System.
- 9.20 Entities must establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of Remote Access allowed.
- 9.21 Entities must authorize Remote Access to an Information System prior to allowing such connections.
- 9.22 When available, entities must deploy MFA for Remote Access to Critical Systems or systems containing Restricted-Use Information.
- 9.23 Remote Access sessions must be encrypted, auditable, and traverse managed access points.
- 9.24 Remote Access sessions to Information Systems that process, store or transmit Restricted-Use Information must be terminated after a period of thirty (30) minutes of inactivity.
- 9.25 Local console sessions on Information Systems that process, store or transmit Restricted-Use Information must be locked after a period of thirty (30) minutes of inactivity.
- 9.26 Authentication must be required to unlock a console session or reestablish a remote session.

## **10.0 SYSTEMS CONFIGURATION STANDARD - CONFIGURATION MANAGEMENT**

- 10.1 Entities must build Information Systems that process, store or transmit Restricted-Use Information from a standard configuration baseline.
- 10.2 The standard configuration baseline must include the specifications of the Information System Components and the security controls for each component.
- 10.3 Entities must maintain an asset inventory of Information Systems' components, update the inventory as changes occur, and review the inventory at least annually.
- 10.4 The asset inventory must also identify and document the relationships between

each of the Information System Components and the ownership of each component.

- 10.5 Collaborative infrastructure, such as video and teleconferencing, must be configured to prohibit remote activation.

#### **CHANGE CONTROL**

- 10.6 Entities must document and adhere to change control processes when making changes to production systems.
- 10.7 Change control requests must include proposed change description, justification, risk assessment, implementation plan, test plan, back-out plan, review and approval.
- 10.8 Entities must maintain a change log for Information Systems containing Restricted-Use Information.
- 10.9 The change log must include:
  - 10.9.1 Date and time of the maintenance
  - 10.9.2 Name and organization of the person performing change
  - 10.9.3 Name of escort, if required
  - 10.9.4 Description of the maintenance performed
  - 10.9.5 List of affected Information System(s) Components or component elements

#### **SYSTEMS PROTECTION**

- 10.10 Entities must implement boundary protection mechanisms with capability to monitor and control network communications.
- 10.11 Within the boundary, entities must create security zones based on data and Information System classification.
- 10.12 Entities must employ malicious code protection mechanisms on systems that contain Restricted-Use Information.
- 10.13 Entities must configure malicious code protection mechanisms to perform weekly scans of files on Information Systems.
- 10.14 Where malicious code protection mechanisms require regular signature or detection engine updates, entities must employ a documented update mechanism that includes testing and installation of applicable updates.

### **11.0 DATA PROTECTION STANDARD**

- 11.1 Entities must employ mechanism(s) to ensure the confidentiality, availability, and integrity of Restricted-Use Information.
- 11.2 Restricted-Use Information that has met the information retention schedule must be removed, destroyed, or deleted in a verifiable manner.
- 11.3 Restricted-Use Information must be protected from unauthorized disclosure.
- 11.4 Entities must use encryption modules, ciphers, or algorithms found within the NIST FIPS 140-2 validated list when encrypting Restricted-Use Information.
- 11.5 Restricted-Use Information when transmitted electronically outside of a secure boundary must be encrypted.
- 11.6 Restricted-Use Information must be encrypted when stored on Portable Electronic Media or Portable Electronic Devices.

#### **MEDIA**

- 11.7 Media containing Restricted-Use Information must be disposed of in accordance

with NIST Special Publication 800-88 – Guidelines for Media Sanitization.

- 11.8 Media that store Restricted-Use Information must be stored securely within a controlled area and physical access to that controlled area must be restricted to authorized personnel.
- 11.9 Media containing Restricted-Use Information must be transported by authorized personnel when leaving a controlled area and must be transported in a manner that ensures appropriate safeguards are applied.

## **12.0 APPLICATION PROCESSING STANDARD**

- 12.1 Entities must define and document principles and procedures for secure application development.
- 12.2 The application element of all Information Systems Components must logically separate user functionality from administrative functionality such that the interface for the one cannot be used to operate the other.

## **13.0 SYSTEMS OPERATIONS STANDARD ASSESSMENT OPERATIONS**

- 13.1 Entities must perform security assessments against all Critical Systems and all Information Systems that process, store or transmit Restricted-Use Information prior to installation in production environments and at least annually thereafter. Security assessments are required to ensure that security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.
  - 13.1.1 Entities must have a documented remediation plan for security issues discovered in security assessments.
  - 13.1.2 Entities must prioritize and establish timelines for implementing corrective actions for all security issues within the remediation plan.
  - 13.1.3 Entities must review all remediation plans and update them at least quarterly.
- 13.2 Entities must perform vulnerability scans against all Information Systems prior to installation into production environments.
- 13.3 Entities must perform vulnerability scans against all network connected Information Systems at least monthly.
- 13.4 Entities must monitor for security alerts and advisories relative to the technologies that are operating within their environments.
- 13.5 Entities must have a documented patch management process.
  - 13.5.1 Patch requirements discovered or resulting from vulnerability scans or continuous monitoring must be addressed expeditiously.
  - 13.5.2 Entities must use a risk-based approach to patch vulnerabilities or deploy mitigating controls when unable to patch vulnerabilities.

## **INTEGRITY OPERATIONS**

- 13.6 Entities must implement controls to ensure that configuration settings are within acceptable parameters.
- 13.7 Entities must implement integrity monitoring on Information Systems that process, store or transmit Restricted-Use Information.
- 13.8 Entities must document and investigate integrity discrepancies.
- 13.9 Entities must validate, then circulate security alerts to appropriate personnel and

ensure corrective action is taken.

## **MAINTENANCE OPERATIONS**

- 13.10 Entities must not operate Information Systems containing Restricted-Use Information without either redundant qualified in-house staff or by contract for vendor managed support.
- 13.11 Entities must configure critical Information Systems to be fault tolerant.
- 13.12 Entities must ensure that critical data is restorable to a known secure state of operations.
- 13.13 Entities must test critical Information System's restoration annually.
- 13.14 Entities must update Information Systems when the support for the components of the Information System are no longer available from the developer, vendor, or the manufacturer.

## **14.0 SYSTEM AUDIT**

- 14.1 Critical Systems and Information Systems that process, store or transmit Restricted-Use Information must be configured such that all user access interactions and system administrators' actions are logged to both the internal system and to an external log repository (not on the local system).
- 14.2 The following data points must be logged:
  - 14.2.1 Event date
  - 14.2.2 Event time
  - 14.2.3 Event source
  - 14.2.4 Event description
  - 14.2.5 Identity of any individual(s) or subject(s) associated with the event(s).
- 14.3 Logs for Critical Systems and Information Systems that process, store or transmit Restricted-Use Information must be stored and maintained for at least 120 days (180 days recommended) on an external log repository or in accordance with other regulatory requirements.
- 14.4 Critical Systems and Information Systems that process, store or transmit Restricted-Use Information must be configured to raise alerts to the system administrative personnel if logging space becomes limited, upon system logging failure, or when suspicious activity is detected within the system logging component.
  - 14.4.1 Entities must actively review and address alerts raised from the logging component.
- 14.5 Information Systems that store logging data must be configured to continue logging by overwriting the oldest logs in the event available space is limited.
- 14.6 Information System logging data must be manually reviewed according to a pre-defined period of time or the logging system configured to automatically raise alerts to the system administrative personnel.
- 14.7 All Production Information Systems must be configured to have time synchronized with authoritative time sources.

## **15.0 INCIDENT RESPONSE STANDARD**

- 15.1 Entities must adopt a documented incident response plan which addresses the following stages: preparing for a security incident, detecting and analyzing a

- security incident; containing a security incident; eradicating and recovering from a security incident; and post incident activities.
- 15.2 Entities must define and document what constitutes a security incident. Security incidents must include intentional and unintentional incidents.
  - 15.3 Entities must define and document a process to track and categorize the severity of all incidents which must drive the associated response, reporting, and communication activities.
  - 15.4 Entities must appoint team members or outside staff/contractors to incident response roles with the following skills:
    - 15.4.1 Communication and coordination
    - 15.4.2 Network analysis
    - 15.4.3 System administration
    - 15.4.4 Security analysis
    - 15.4.5 Legal counsel
    - 15.4.6 Privacy
  - 15.5 Entities must ensure that Incident Response (IR) training for all IR team members has been completed within ninety (90) days of initial assignment of the individual to the IR team. In the event the entity contracts for IR services, the entity must receive assurance that the contractor has the necessary skills and training to carry out incident response services.
  - 15.6 Entities must ensure annual IR training for all IR team members as identified above.
  - 15.7 Entities must annually conduct IR operations testing using classroom, tabletop exercises, or live incidents.
  - 15.8 Entities must conduct an exercise recreating a significant incident scenario that requires an operations-based functional exercise (or a major live incident) to validate the IR plan, procedures, and agreements, to clarify roles and responsibilities, and to identify resource gaps once every five (5) years.
  - 15.9 Entities must have dedicated tools and documented processes to conduct incident response activities. If the entity does not have the tools, resources, or expertise, then the entity must identify a service provider to assist with incident response activities.
  - 15.10 Entities must have a documented incident communications strategy to provide adequate and timely communication to all appropriate stakeholders.
  - 15.11 For significant security incidents, entities must perform a post-incident review within a reasonable timeframe upon containment, to document lessons learned and to improve Information System protection and incident response capabilities in the future. Post-incident review documentation must be communicated to entity leadership.

## **16.0 PHYSICAL SECURITY STANDARD DATA CENTERS**

- 16.1 Entities must restrict physical access to data centers that process, store or transmit Restricted-Use Information to authorized personnel only.
- 16.2 Entities must maintain a list of all authorized personnel with physical access to data centers that process, store or transmit Restricted-Use Information.
  - 16.2.1 This list must be reviewed and updated annually.

- 16.2.2 This list must be updated as user access privileges change.
- 16.3 Entities must require authorized personnel to authenticate themselves prior to entry to data centers that process, store or transmit Restricted-Use Information.
  - 16.3.1 Visitors to data centers that process, store or transmit Restricted-Use Information must be escorted by authorized personnel at all times.
  - 16.3.2 Entities must log all visitor access to data centers that process, store or transmit Restricted-Use Information.
- 16.4 Data centers must implement physical environmental controls that mitigate or prevent damage from water, fire, temperature, and humidity for Information Systems that process, store or transmit Restricted-Use Information.
- 16.5 Entities must ensure sufficient power protection is available for critical Information Systems to perform an orderly shutdown.

## **17.0 PERSONNEL SECURITY STANDARD ACCEPTABLE USE**

- 17.1 Acceptable use policies must restrict the use of all equipment and access to public and private networks to approved entity related operations.
- 17.2 Entities must require users to acknowledge adherence to the entity acceptable use policy prior to being granted access to Information Systems.
- 17.3 Entities must include policy violation consequences in their acceptable use policies.
- 17.4 Entity acceptable use policies must assert that violations will be investigated as a security event.

### **PERSONNEL OPERATIONS**

- 17.5 Entities must retain a form of acknowledgement of the acceptable use policy.
- 17.6 Entities must assign all users to a user categorization based upon their role and least privilege.
- 17.7 Entities must assign Information System authorizations to users based on user categorization and Information System classification.
- 17.8 Entities must revoke system access or eliminate unnecessary permissions for user accounts as users are transferred, terminated, or their role has changed.
- 17.9 Entities must recover all property that has been assigned to terminated personnel.

## **18.0 SECURE PURCHASING/ACQUISITION STANDARD**

- 18.1 Entities must include system security requirements with all Requests for Proposal, Information, Quotation (RFP, RFI, RFQ) and all contracts.
- 18.2 All acquisition documents must specify the entity's security requirements and allow for the validation of those security requirements.

## **19.0 RESPONSIBILITIES:**

- 19.1 The State of Kansas Information Technology Security Council (ITSC) is responsible for the maintenance of these standards.
- 19.2 These standards will be reviewed by the ITSC at least every three (3) years.
- 19.3 Entities must ensure verifiable compliance with these requirements no later than three (3) months from the effective date. Entities should ensure Variances or Exceptions are in place, in accordance with this standard, for any requirements they cannot meet.

Don Brownlee, Executive Director

Laura Kelly, Governor

<b>Subject</b>		<b>Number</b>	<b>Draft #</b>
<b>CYBERSECURITY POLICY NEWS LETTER AND SECURITY ALERTS</b>		<b>2020-02</b>	<b>(4)</b>
<b>Adopted</b> September 11, 2020	<b>Last Revision</b> March 13, 2020	<b>Rescinds</b>	
<b>Commission Authorization</b>			
Chairman Brandon Jones		Date	

## I. Purpose/Background

This policy is promulgated pursuant to the Kansas Cybersecurity Act of 2018, K.S.A. 75-7236, et seq.

Cybersecurity standards enhance security and manage risk in many essential ways. Standards establish common security practices and the capabilities needed for such practices. This Cybersecurity Policy will allow the agency to better adapt to changing threats.

Protecting agency data is a shared effort. Individuals with access to agency data are responsible for accessing, storing, and processing data on systems that have appropriate security controls in place. KRG C Cybersecurity Policies 2020-03 through 2020-24 further detail these requirements.

This document defines the minimum security standards required for any electronic device or cloud service that may be used to access, store, or process (input, output, transmit, receive, display, calculate, etc.) sensitive information that is owned or used by KRG C.

## II. Introduction

The KRG C is dedicated to maintaining the security and privacy of the data in its custody. The KRG C will do so by maintaining confidentiality, integrity, and accessibility. The agency will train and disseminate information on the validation of security information to staff members in compliance with ITEC 7230A § 13.9. The agency's Information Technology & Cybersecurity unit (IT&CS) shall circulate this information to staff members.

### **III. Policy**

The agency shall disseminate information through a monthly newsletter, issued on the 15<sup>th</sup> of every month, which will be focused on cybersecurity issues. The newsletter will be distributed at least once per month. In instances in which information needs to be disseminated before the next issue, a supplemental newsletter shall be sent via email with a Microsoft Outlook email Read notice.

The agency will maintain a copy of all disseminated newsletters, and IT&CS will create an entry in the “Dissemination Log” (Appendix A).

If IT&CS obtains any information that indicates an imminent threat to the agency, it will take immediate action to mitigate that threat. IT&CS shall send memorandums or emails to any staff who are necessary to assist in reducing the threat. IT&CS will create a timeline of actions that are necessary to address the threat. That timeline will be monitored by the Director of IT&CS and the agency’s Executive Director. If something must be purchased to address a cybersecurity threat, a purchase order shall be given immediately to the Director of IT&CS who shall oversee obtaining any necessary resources.



Don Brownlee, Executive Director

Laura Kelly, Governor

<b>Subject</b>		<b>Number</b>	<b>Draft #5</b>
<b>CYBERSECURITY POLICY INTELLECTUAL PROPERTY</b>		<b>2020-04</b>	
<b>Adopted</b> September 11, 2020	<b>Last Revision</b> March 13, 2020	<b>Rescinds</b>	
<b>Commission Authorization</b>			
Chairman Brandon Jones	Date		

### **I. Purpose/Background**

The purpose of this policy is to establish the responsibilities of all staff members to prevent copyright infringements and comply with the Digital Millennium Copyright Act (DMCA).

### **II. Introduction**

- A. Unauthorized replication of software is illegal. Copyright law protects software writers and publishers. Persons possessing illegal copies of software may be subject to criminal and civil legal action by the publisher.
- B. Unauthorized copying of software by individuals that is condoned by this agency can harm the agency and stunt imagination and growth in the writing of programs and coding. Unauthorized copying and use of any intellectual property could cause the individual and this agency to incur a legal liability.
- C. Unauthorized copying of software can deprive developers of a fair return for their work, increase prices, reduced level of future support and enhancement, and inhibited development of new software products.

### **III. Authority**

The Kansas Cybersecurity Act, K.S.A. 75-3236, *et seq.*, authorizes the Office of Information Technology Services (OITS) to establish statewide technology policies which include technology and security standards. These mandated policies are developed and approved by the Kansas Information Technology Executive Council. They were developed, approved, and published through IETC 7230A. Section 6.0 of this document states that intellectual property will be included in an agency's assets and requires the assignment of a Trustee and Custodian to protect such assets.

#### **IV. Policy**

Access to KRGC networks and computer systems, including their purchased and leased intellectual property, is granted subject to KRGC policies and local, state, and federal laws. Appropriate use shall always be legal and ethical. Users shall demonstrate respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy, freedom of speech, and freedom from intimidation, harassment, and unwarranted annoyance.

- A. The Director of Information Technology and Cybersecurity shall be the Data Trustee for the agency's intellectual property, most of which is information technology purchased by the Information Technology (IT) department. Additionally, most intellectual property infringements occur over the internet or the intellectual property is accessed through a computer system. The Data Trustee shall appoint a custodian.
- B. Use of Peer-to-Peer (P2P) file sharing applications for the unauthorized acquisition or distribution of copyrighted or licensed material is prohibited on any KRGC computer or network. P2P file sharing applications commonly used for these illicit purposes shall not be installed on any agency computer and technological deterrents will be used to detect and block their use on the agency network. The unauthorized acquisition or distribution of copyrighted or licensed material, including unauthorized peer-to-peer file sharing, may subject individuals to civil and criminal liabilities.
- C. Unauthorized copying of software or circumventing of licensing is prohibited.
- D. The Data Trustee shall maintain and provide a list of P2P file sharing applications commonly used for unauthorized acquisition or distribution of copyrighted or licensed material. These include, but are not limited to the following providers: Ares, BitTorrent, eDonkey aka eMule, and Gnutella aka LimeWire. These and other similar applications shall not be installed on agency computers and will be blocked on the network.
- E. All staff members shall comply with federal copyright laws and shall obtain permission for use of copyrighted material unless the use can fairly and reasonably be interpreted as "fair use" under the U.S. Copyright Office definition which is provided in Appendix A. If staff are unsure of their understanding of any part of this policy, staff are encouraged and expected to request further information and resources to determine how to comply with federal copyright law.
- F. Staff who willfully disregard this policy could individually be at risk of adverse legal action. In such cases, the agency may refuse to defend the employee named in any litigation and the employee may be held personally liable.
- G. To ensure licensing safeguards, remote access control procedures are provided. Only KRGC equipment can be used for remote access so that access is not given to computers that are not licensed. This restriction does not apply to authenticated user

access to web applications like the KRGC Intranet, Webmail or systems designed for public access.

## APPENDIX A FAIR USE EXPLAINED

Fair use is a legal doctrine that promotes freedom of expression by permitting the unlicensed use of copyright-protected works in certain circumstances. Section 107 of the Copyright Act provides the statutory framework for determining whether something is a fair use and identifies certain types of uses—such as criticism, comment, news reporting, teaching, scholarship, and research—as examples of activities that may qualify as fair use. Section 107 calls for consideration of the following four factors in evaluating a question of fair use:

1. *Purpose and character of the use, including whether the use is of a commercial nature or is for nonprofit educational purposes:* Courts look at how the party claiming fair use is using the copyrighted work, and are more likely to find that nonprofit educational and noncommercial uses are fair. This does not mean, however, that all nonprofit education and noncommercial uses are fair and all commercial uses are not fair; instead, courts will balance the purpose and character of the use against the other factors below. Additionally, “transformative” uses are more likely to be considered fair. Transformative uses are those that add something new, with a further purpose or different character, and do not substitute for the original use of the work.
2. *Nature of the copyrighted work:* This factor analyzes the degree to which the work that was used relates to copyright’s purpose of encouraging creative expression. Thus, using a more creative or imaginative work (such as a novel, movie, or song) is less likely to support a claim of a fair use than using a factual work (such as a technical article or news item). In addition, use of an unpublished work is less likely to be considered fair.
3. *Amount and substantiality of the portion used in relation to the copyrighted work as a whole:* Under this factor, courts look at both the quantity and quality of the copyrighted material that was used. If the use includes a large portion of the copyrighted work, fair use is less likely to be found; if the use employs only a small amount of copyrighted material, fair use is more likely. That said, some courts have found use of an entire work to be fair under certain circumstances. And in other contexts, using even a small amount of a copyrighted work was determined not to be fair because the selection was an important part—or the “heart”—of the work.
4. *Effect of the use upon the potential market for or value of the copyrighted work:* Here, courts review whether, and to what extent, the unlicensed use harms the existing or future market for the copyright owner’s original work. In assessing this factor, courts consider whether the use is hurting the current market for the original work (for example, by displacing sales of the original) and/or whether the use could cause substantial harm if it were to become widespread.

Although these are good guidelines, there are other considerations a court could weigh in on a fair use question, depending on the circumstances. These are handled on a cases-by-case basis, and are dependent on the specific case. There is no formula to ensure that a predetermined percentage or amount of work, or specific number of words, lines, pages, copies, may be used

without permission. If a KRGC staff member needs to use or reproduce copyrighted material, the staff member shall consult with their supervisor and the legal department before doing so.

Don Brownlee, Executive Director

Laura Kelly, Governor

<b>Subject</b>		<b>Number</b>	<b>Draft #3</b>
<b>CYBERSECURITY POLICY DEFINITIONS</b>		<b>2020-05</b>	
<b>Adopted</b>	<b>Last Revision</b>	<b>Rescinds</b>	
September 11, 2020	April 29, 2020	N/A	
<b>Commission Authorization</b>			
Chairman Brandon Jones	Date		

**I. Purpose/Background**

- A. The purpose of all KRGC cybersecurity policies is to fulfill the requirements of the Kansas Cybersecurity Act of 2018.
- B. The purpose of this Definitions policy is to be a one-location reference for defining terms and listing any applicable authority from state statutes, ITEC policy, or KRGC interpretation. Terms that are acronyms are spelled-out and defined. These definitions apply to all KRGC Cybersecurity Policies that fulfill the requirements of the Kansas Cybersecurity Act of 2018.

**II. Policy Definitions**

TERM	DEFINITION
<b>“#s”</b>	
<i>121, one-to-one</i>	The philosophy in internet e-commerce that treating each customer as a special individual is a more successful approach than treating customers as a group of similar individuals.
<i>404 error page</i>	The webpage that is served to users when they try to access a page that is unavailable.
<i>80</i>	Occasionally a mysterious 80 can appear on the name of a web server that is handling a request for webpages. This is a bit of technical text showing when it likely should not.

**TERM****DEFINITION****“A”**

***Access control list, ACL***

A set of rules in a network device, such as a router, that controls access to segments of the network. A router with an ACL can filter inbound and/or outbound network traffic similar to a firewall but with less functionality.

***Access point***

Provides wireless access to a network. Devices connected to an access point can communicate with other devices on the network. They may also connect to the internet if the access point is linked to an internet connection, which is commonly the case. Access points that use Wi-Fi are also called base stations.

***Acceptable use policy, AUP***

A policy that a user must agree to in order to be provided with access to a network or to the internet.

***Account archived***

Accounts that have not been used for a certain period of time are off-loaded via long-term storage solutions.

***Account disabled***

Accounts that are in an unusable state and can only be made usable again through an administrative action.

***Account locked***

Accounts that are not useable until either an administrator resets a token or the end-user resets the token through one of the forgotten password self-service functions.

***Account promotion***

The process of changing the security level of an account from a lower level to a higher level using applicable identification methods.

***Act***

KSA 75-7237(a) defines "act" as the Kansas Cybersecurity Act.

**TERM****DEFINITION*****Active Directory,  
AD***

A directory service that stores data as objects, which is either resources, such as printers or computers, or security standards, such as users or groups. Active Directory categorizes objects by name and attributes. The main service in Active Directory is Domain Services (AD DS), which stores directory information and handles the interaction of the user with the domain. AD DS verifies access when a user signs into a device or attempts to connect to a server over a network. AD DS controls which users have access to each resource.

***Address of record***

An individual's official location that is on record with a trusted or authoritative entity such as a government agency, the individual's employer, financial institution, or utility company. The address of record always includes an individual's residential street address and may also include the mailing address of the individual.

***Advanced persistent  
threat, APT***

An attack that is deployed by cyber-criminals who have a high level of expertise and important resources to infiltrate a network. They usually use this type of attack to target large organizations seeking to retrieve economic or financial information. In some cases, they try to use this form of attack to stop or block an organization's program or agenda. Because an advanced persistent threat is executed over long periods of time, it is difficult for average users to detect and block and requires a specialized security program or a team of experts to address.

***Adverse event***

An event that indicates or produces an actual or potential negative consequence to state of Kansas information technology (IT) systems. These include attempted or actual system crashes, network packet floods, unauthorized use or disclosure, defacement of a webpage, and execution of malicious code. The state of Kansas rates low and medium intrusion detection reports as undesirable events. High intrusion detection reports are to be considered cybersecurity incidents. Documented and verified adverse events are incidents.

**TERM****DEFINITION**

<i>Adware</i>	A software application that is often included with a program that is offered at low cost or no charge. Adware displays advertising banners while running a program by including additional code that delivers the ads, which can be displayed through pop-up windows or through a bar that appears on the computer screen. Often includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge. Is a type of spyware that gathers information about a user's browsing habits and displays targeted or contextual advertisements.
<i>After action report</i>	A document containing findings and recommendations from a cybersecurity incident, exercise, or test.
<i>Agency</i>	The Kansas Racing and Gaming Commission (KRGC).
<i>Agency network</i>	Any part of the KRGC's data and information network physically located in Topeka, Dodge City (Boot Hill Casino), Kansas City (Hollywood Casino at Kansas Speedway), Mulvane (Kansas Star Casino), Pittsburg (Kansas Crossing Casino), or elsewhere within the state.
<i>Alphanumeric</i>	Describes the combined set of all letters in the alphabet and the numbers 0 through 9. Grouping letters and numbers together is useful because many programs treat them identically, but separate from punctuation characters. For example, most operating systems allow users to use any letters or numbers in filenames but prohibit many punctuation characters.
<i>Alphanumerish</i>	The shorthand typing language that has developed from computer users' habit of substituting numerals for letters and substituting both letters and numerals for words or word parts.
<i>Alt attribute</i>	Used in an <img> tag to describe the image.

**TERM****DEFINITION*****Angler exploit kit***

Emerged in 2013 and is one of the most famous and sophisticated exploit kits in the cyber-criminal community. Features aggressive tactics to avoid being detected by security products and is capable of exploiting a vast array of software vulnerabilities in order to infect unsuspecting victims with malware. Because it's usually spread through drive-by downloads, Angler is extremely difficult to detect and can infect users without any interaction. It also features file-less infection capabilities and is able to deliver a variety of payloads, including ransomware, Trojans, rootkits, and backdoor Trojans. Cyber criminals do not need advanced technical skills to use it, and it is a constantly evolving threat.

***Anomaly-based intrusion detection***

A new technology that protects systems or networks against malicious and cyber-criminal activities using a heuristics-based detection, and less the classic signature-based methods. Because this detection type is newer, it delivers a high number of false positives. The challenge is that a system must recognize abnormal activities and flag them as dangerous, but it continues to be difficult to instruct a computer on what normal usage of the system is.

***Anonymizing proxy***

A method of hiding a user's online activity and/or making the activity very difficult for third parties, like governments that censor the internet, to disclose. Proxy servers act like an intermediary connection between the computer and the final target. From an outsider's point of view, the proxy servers access those web locations and hide the computer's IP address. They are often used to access internet content under strict censorship.

***Anti-malware***

Refers to a number of software programs and applications that are capable of detecting and removing malware from individual systems or from larger networks. Though the term is usually used in connection with classic antivirus products, the anti-malware abilities can include anti-spyware, anti-phishing, or anti-spam solutions. The term has expanded to name specialized software that fights data stealing malware used by online criminals.

***Anti-spam***

Techniques that are employed by special software programs to fight spam, which is unsolicited e-mail. Spam is one of the main ways to deliver the most dangerous malware.

<b>TERM</b>	<b>DEFINITION</b>
<i>Anti-spoofing</i>	Techniques that are used to stop DDoS (Distributed Denial-of-Service) attacks. To conduct these attacks, hackers spoof IP addresses from where they send a large number of requests. When the website server attempts to reply to the requests, it gets stalled by waiting to access servers that actually do not exist. The source of these attacks is difficult to detect and the only available solution is to use a software that can detect these fake IP addresses and refuse the requests.
<i>Antispyware software</i>	Used in detecting and blocking spyware attempts. Spyware is a type of software that allows advertisers or online criminals to discover personal data from a computer without the user's permission. (See further information in the Spyware definition below.)
<i>Antivirus, anti-virus, AV</i>	Software designed to prevent, detect, and remove viruses from a computer. Once installed, most antivirus programs run in the background, scanning new files for viruses and performing regular system checks. Antivirus programs can scan individual files or folders directly. The software operates by checking files against a database of virus definitions, which contain signatures of known viruses. The software must be promptly and continuously updated. Typically, if a file contains a virus, the program will quarantine the file, making it inaccessible thereby removing the threat. The program may also mark the file for deletion. While antivirus software primarily scans for viruses, most modern antivirus programs also scan for other types of malware.
<i>Applicant</i>	A person who has applied for a license or certificate and the license or certificate issuance procedure is not yet completed.
<i>Application owner</i>	The point of contact for a KRGC Application.
<i>Assistive technology devices</i>	Any item, piece of equipment, or product system, whether acquired commercially, modified, or customized, that is used to increase, maintain, or improve functional capabilities for individuals with disabilities.
<i>Atmos</i>	A form of financial malware that emerged from Citadel (which is based on the Zeus leaked code). Atmos has been active since late 2015 but there has been a significant increase of its use since April 2016.

TERM	DEFINITION
<i>Attack, cyber attack</i>	Can come in many forms and may target average individuals or large corporations. Attacks usually attempt to steal financial and commercial information, disclose important data, destroy data, or block access to a server.
<i>Attack signature</i>	A unique piece of information that is used to identify a particular cyber attack aimed at exploiting a known computer system or a software vulnerability. Attack signatures include certain paths used by cyber criminals during their malicious compromise attempts. These paths can define a certain piece of malicious software or an entire class of malware.
<i>Attack vector</i>	A method of attacking a system, for example sending emails with infected links, posting infected links on a webpage, or leaving an infected USB drive in a parking lot with the hope that someone plugs it into a computer so that it can upload a virus.
<i>Authenticated scan</i>	A credential based scan that provides sufficient access to allow the vulnerability scan engine to scan the operating system and all applications running on the system.
<i>Authentication</i>	<p>The process of verifying one's digital identity. For example, when someone logs into webmail, the password verifies that the person logging in is the owner of the user ID. This verification process is called authentication. Authentication requires users to have one or more of the following to gain access to a system:</p> <ul style="list-style-type: none"> <li>• Something one knows (e.g. user ID, password, memorized personal identification number (PIN), or passcode)</li> <li>• Something one has (e.g. a one-time password authentication token, smart card)</li> <li>• Something one is (e.g. fingerprint, retina scan)</li> </ul>
<i>Authentication method</i>	The authentication mechanism used at the time of user account login.
<i>Authentication token</i>	An item used for the “what one has” authentication factor. The token typically provides a second password or authentication key.
<i>Authorization</i>	Access privileges granted to a user, program, or process; or the act of granting those privileges.
<i>Automated attendance &amp; leave system</i>	A computer-based application that facilitates the preparation, review, auditing, and reporting of employees' attendance and leave accrual balances, and processes appropriate payroll transactions.

**TERM****DEFINITION**

***AutoRun worm*** Malware programs that use the Windows AutoRun feature to launch automatically when the device, usually a USB drive, is plugged into a PC. A similar technology, AutoPlay has been exploited to deliver the Conficker worm into PCs. Microsoft has changed its settings so that AutoRun is off for new systems so the use of these worms should decrease or disappear in the future.

***Availability*** The extent to which information is operational, accessible, functional, and usable upon demand by an authorized entity such as a system or user.

**“B”**

***Business Continuity Plan, BCP*** A set of documents, instructions, and procedures which enable a business to respond to accidents, disasters, emergencies, and/or threats without any stoppage or hindrance in its key operations. Also called a business resumption plan, disaster recovery plan, or recovery plan.

***Backdoor Trojan*** A method of taking control of a system without permission. Typically, a backdoor Trojan poses as a legitimate program and is spread through phishing campaigns by fooling users into clicking on a malicious link or accessing malware on a website. Once the system is infected, the Trojan can access sensitive files, send and receive data online, and track the browsing history. To avoid this type of infection, the system should be kept up-to-date with the latest patches and have strong anti-malware protection.

***Backup*** An exact copy of a computer's files, system files, or any other system resources one needs to protect. This precaution is necessary for all types of unpredictable events, like a system crash, when files are inadvertently removed or lost, when files become infected, or a system is blocked by ransomware. The backup should be independent from the system and only used when necessary.

***Bandwidth*** A measurement of the amount of data that can be transmitted over a network at any given time. The higher the network's bandwidth, the greater the volume of data that can be transmitted.

***Baseline security*** A set of basic measures and objectives that any service or network system should be able to meet. This baseline methodology is usually a set of security steps that are implemented and imposed by an organization's IT cybersecurity staff.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Baselining</i></b>	Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.
<b><i>Best practice guideline</i></b>	A case study and/or analysis which provides a benchmark for good business and IT practices to achieve a desired result. The analysis or case study highlights one or several proposed products, technology fields, analytical methodologies, or IT solutions which constitute a good approach for other entities pursuing similar solutions. While not mandatory, best practices guidelines are intended to be informational, to facilitate knowledge transfer, and to shorten the learning curve for other entities addressing common technology issues.
<b><i>Biometrics</i></b>	Refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or retinas.
<b><i>Bit</i></b>	A binary digit (either 0 or 1). The most basic unit of data that can be recognized and processed by a computer.
<b><i>Bitrate</i></b>	The number of bits used per unit of time to represent a continuous medium such as audio or video after source coding (data compression). Bitrate corresponds to the term digital bandwidth consumption. While often referred to as "speed," bitrate does not measure distance over time but quantity over time.
<b><i>Blackhat hacker</i></b>	Skilled computer users with malicious intent, they seek to compromise the security of a person or organization for personal gain. Blackhat hackers frequently specialize in malware development, spam delivery, exploit discovery, DDoS attacks, and more. Some Blackhat hackers do not use the malware they develop or the exploits they discover. Instead, they sell their malware or knowledge to the highest bidder. Favorite targets include financial information (such as credit card data or bank accounts), personal information (like email accounts and passwords), and sensitive company data (such as employee/client databases).
<b><i>Blacklisting</i></b>	Organizing a list of senders that have conducted malicious activities, like phishing or spam. A blacklist can also contain applications or programs that should not be launched on a system. For a firewall solution, blacklisting blocks IP addresses that the system should not connect for safety reasons.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Blended threat</i></b>	A widely-used term to describe an online attack that spreads by using a combination of methods, like worms, Trojans, viruses, and other malware. This combination of malware elements using multiple attack vectors increases the likelihood of damage and is difficult for individual systems and networks to defend against.
<b><i>Bloatware</i></b>	A derogatory name for unwanted pre-installed software applications on a new computer.
<b><i>Blog</i></b>	Originated from the term weblog, a webpage that contains journal-like entries and links that are updated regularly for public viewing.
<b><i>Bluetooth</i></b>	A wireless networking technology that allows users to send voice and data from one electronic device to another via radio waves.
<b><i>Board of Trustees</i></b>	All of the Data Trustees who, as a group, have the ability to audit and evaluate cybersecurity policies and procedures. The Board answers to the Executive Director. The Board performs tasks such as annually evaluating the physical security procedures for the agency.
<b><i>Boot sector</i></b>	A dedicated section of a hard disk or other storage device that contains data used to boot a computer system. Includes the master boot record, which is accessed during the boot sequence.
<b><i>Boot sector malware</i></b>	Malware that is capable of replicating the original boot sector of the system, so that during boot-up the malware can become active. By doing this, the boot kit in the boot sector manages to hide its presence before the operating system can load. This advantages the malware because it is loaded before the operating system which includes the anti-malware solution. Because the malware loads before the security solution, the malware can even disable the security solution. This malware is typically difficult to remove.
<b><i>Bot, internet bot, web bot</i></b>	Software programs that perform automated tasks and specific operations. Though some bots serve harmless purposes in video games or online locations, there are a number of bots that can be employed in large networks, from where they can deliver malicious ads on popular sites or launch distributed online attacks against a number of designated targets.
<b><i>Botnet</i></b>	A network of compromised machines that can be remotely controlled by an attacker. Due to their immense size (tens of thousands of systems that can be linked together), they pose a severe threat to the government's IT infrastructure.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Breach</i></b>	Any illegal or unauthorized access to a computer system that causes damage or has the potential to cause damage. K.S.A. 75-7237(b) defines a breach as: “unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of an executive branch agency does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use. It can also be non-digital. . . .”
<b><i>Brochureware</i></b>	Web sites or pages that are produced by taking an organization's printed brochure and translating it directly to the web without regard for the possibilities of the new medium.
<b><i>Browser hijacking</i></b>	The process of changing the default homepage or search engine on a web browser by a malicious program without the user’s permission. The user may notice that the changes cannot be reversed and a security tool must be used to combat this type of software. Not considered a serious threat to the overall security of a system, but should be addressed quickly because it affects web browsing.
<b><i>Brute force attack</i></b>	A trial-and-error method of attack to obtain information (such as a password or PIN) in which the attacker attempts entry by using all possible characters for the PIN or password until entry is gained.
<b><i>Buffer</i></b>	A temporary holding area for data while it's waiting to be transferred to another location. Usually located in the RAM. The concept of the buffer was developed in order to prevent data congestion from an incoming to an outgoing port of transfer.
<b><i>Buffer overflow</i></b>	Occurs when a program or an application tries to store excess data in a buffer and that extra information overflows into other parts of the computer's memory. This overflow was exploited by hackers and can lead to unauthorized code running or system crashes.
<b><i>Bug</i></b>	A software flaw that produces an unexpected result that may affect the system's performance. Bugs can cause system crashing or freezing. The primary security concern is that bugs may allow hackers to bypass access privileges or retrieve sensitive data from a network.
<b><i>Bulk encryption</i></b>	A set of security protocols that provide the means of encrypting and decrypting data transmissions in order to protect against security breaches and online theft.

**TERM****DEFINITION**

***Bulk load registration***

An account creation process used for the initial loading of a large number of user accounts.

***Business analysis and risk assessment***

Identifying and evaluating various factors relevant to the selection of an electronic signature for use or acceptance in an electronic transaction. Such factors include, but are not limited to, relationships between parties to an electronic transaction, value of the transaction, risk of intrusion, risk of repudiation of an electronic signature, risk of fraud, functionality and convenience, business necessity and the cost of employing a particular electronic signature process.

***Business impact analysis, BIA***

An important element of an organization's business continuity plan that detects vulnerabilities and analyzes their operational and financial impact on the overall business plan. According to the analysis, strategies are planned to minimize the detected risks.

***Business owner***

Person who authorizes a project or the person's designated employee.

***Byte***

A group of adjacent binary digits that a computer processes as a unit to form a character such as the letter "C". A byte consists of eight bits.

**“C”**

***Cybersecurity Incident Response Team, C-SIRT***

The individuals trained for and assigned to handle any cybersecurity event at KRGC. They are responsible for duties defined in ITEC 7230A §15.0 and all subsections. See KRGC policy 2020-15.

***Cache***

Technology used to store data and allow future requests to be served at a higher speed. This high-speed storage method is usually used for webpages and online documents, like HTML pages and images, to increase the loading speed and avoid unwanted lag.

***Cache cramming***

A technique to trick a browser into running malicious Java code from the local disk, instead of the internet. The execution of local code (which runs with less permissions) enables online criminals to access the target computer.

<b>TERM</b>	<b>DEFINITION</b>
<i>Catfishing</i>	An impersonator fools a victim into believing there is a genuine relationship between the two, carried out through text or phone but never in person. Typically, the impersonator will ask for a large favor, usually monetary, with the promise that after the favor the two will finally meet face to face. After the favor is completed, the impersonator still gives reasons to not meet and continues trying to extract money from the victim.
<i>Censorware</i>	A term used pejoratively to describe software that filters out undesirable web sites or content.
<i>Central processing unit, CPU</i>	The part of a computer in which operations are controlled and executed.
<i>Certificate authority, CA</i>	An entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key.
<i>Certified copy</i>	A duplicate of an original official document, certified as an exact reproduction by the officer responsible for issuing /keeping the original document.
<i>Chain of custody</i>	Protection and documentation of the handling of evidence by each responsible party to prevent loss, breakage, alteration, or unauthorized handling. The process includes properly securing, identifying, and dating the evidence by marking it.
<i>Chargeware</i>	A form of scamming usually associated with online porn. A method to manipulate the user into signing up for unclear terms and conditions that overcharge a credit card and makes it difficult to unsubscribe.
<i>Checksum</i>	A simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message. The receiving station then applies the same formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been garbled.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Chief Information Officer, CIO</i></b>	The person who is responsible for the information technology system in KRGC or the executive branch. Job responsibilities include planning the technology architecture, aligning corporate network to the business, and developing a secure financial management system for the organization.
<b><i>Chief Information Security Officer, CISO</i></b>	Under K.S.A. 75-7237(c), CISO is the Chief Information Security Officer for the state government's executive branch.
<b><i>Chief Security Officer, CSO</i></b>	A top-level executive in charge of ensuring the security of a company's personnel, financial, physical and digital assets. A CSO has both security and business oriented objectives, as he/she is responsible for aligning cyber protection with the company's business goals. All security strategies, tactics, and programs have to be directed and approved by the CSO.
<b><i>Citadel</i></b>	A form of financial malware which emerged in 2012, after the source code for the infamous ZeuS malware was leaked online. Because the code was open source, cyber criminals started improving it to get newer, more sophisticated and stealthier malware types. Just like ZeuS/Zbot, Citadel aims to retrieve confidential information, especially banking and financial information, from victims. Citadel can also run different types of malware, such as ransomware or scareware, which makes it advanced toolkit for cyber criminals.
<b><i>Claimant</i></b>	A party whose identity is to be verified using an authentication protocol.
<b><i>Classified National Security Information</i></b>	Information that has been determined by the federal government to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. There are three classifications - confidential, secret, and top secret.
<b><i>Clear</i></b>	The lowest level of sanitizing data. Under NIST 800-88 it applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

<b>TERM</b>	<b>DEFINITION</b>
<i>Clear gif</i>	A graphic with a unique identifier, similar to a cookie, used to track the online movements of users. Clear gifs are also known as pixel tags, web beacons, or web bugs.
<i>Clear text</i>	Any message or text that is not rendered unintelligible through an encryption or hashing algorithm.
<i>Click-through</i>	A message on a user's computer screen, requiring that the user respond to a question and, as a result, provide information by clicking on an icon.
<i>Client-side image map</i>	HTML code delivered to the browser that provides coordinates to hot spots users may click on inside a given image.
<i>Clock cycle</i>	Sometimes stated as simply a cycle. A single electronic pulse of a central processing unit (CPU). During each cycle, a CPU can perform a basic operation such as taking an instruction, accessing memory, or writing data. Since only simple commands can be performed during each cycle, most CPU processes require multiple clock cycles.
<i>Clock speed</i>	The rate at which a processor can complete a processing cycle. Typically measured in megahertz or gigahertz. One megahertz is equal to one million cycles per second, while one gigahertz equals one billion cycles per second. This means a 1.8 GHz processor has twice the clock speed of a 900 MHz processor.
<i>Code injection</i>	The code injection technique is usually used by online attackers to change the course of the execution of a computer program. This method is used by online criminals to spread malicious software by infecting legitimate websites with malicious code.
<i>Cold site</i>	A backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, exist and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the building might have a network infrastructure and a room ready to act as a server room. Typically, cold sites provide the physical location and basic services. SOURCE: CNSSI-4009 Through NIST IR7298 Revision 2.
<i>Collaborative computing device</i>	May include, but are not limited to, networked white boards, cameras, and microphones that are connected to KRGC IT systems for the purpose of conducting government business collaboratively.

TERM	DEFINITION
<i>Collect</i>	To store information, including via cookie technology, in order to retrieve it at a later time to initiate communication with or make determinations about the person who is the subject of such information.
<i>Command and control center, C&amp;C</i>	A network server that controls a large network of compromised systems. The malicious server is used by hackers to send and receive commands from and to the infected computers. Using this type of network, hackers can launch distributed denial-of-service attacks by instructing the computers to perform the same action.
<i>Commission</i>	The Kansas Racing and Gaming Commission.
<i>Commissioner</i>	An individual who serves on the Commission.
<i>Component test</i>	A test of individual hardware and software components or groups of related components.
<i>Comprehensive test</i>	A test of all systems and components that support a particular IT plan, such as a contingency plan or computer security incident response plan.
<i>Compromise</i>	The unauthorized disclosure, modification, substitution, or use of sensitive information, or the successful action to invade system by evading its security. For example, a computer has been compromised when a Trojan virus has been installed.
<i>Compromise of integrity</i>	Any unauthorized modification of information or data.
<i>Computer abuse</i>	The unethical use of a computer to launch online attacks, like phishing, malware delivery campaigns, sabotage, and cyberwar activities.
<i>Computer forensics</i>	The practice by which digital data is collected and analyzed for legal purposes. The main goal is to identify, analyze, and present facts about digital information. The conclusions can be used in investigations of cyber-crime or for civil proceedings.
<i>Computer network defense, CND</i>	The defensive measures taken to protect information, information systems, and networks from threats.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Computer security incident</i></b>	Defined by NIST as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Also defined as any event that adversely affects the confidentiality, integrity, or availability of a system and its data.
<b><i>Confidential data</i></b>	Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need to know. See KRGC's Data Classification and Security Policy (2020-06) for an expanded definition and examples.
<b><i>Confidentiality</i></b>	A set of rules or an agreement that limits access or restricts that access to certain types of information. When such agreement is in place, information is disclosed to only those who are authorized to view it.
<b><i>Consolidated log infrastructure</i></b>	The hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data.
<b><i>Control</i></b>	An action taken to enhance the likelihood that established goals or objectives will be achieved (in the context of this policy, generally an action taken to reduce risk.)
<b><i>Control cell</i></b>	A central location for exercise coordination, typically in a separate area from the exercise participants.
<b><i>Cookie</i></b>	A small text file which is placed on a computer when a user visits a website that allows the website to keep track of visit details and store a user's preferences. These cookies were designed to be helpful and increase the website speed the next time a user accesses that location. They are also very useful for advertisers who can match ads to a user's interests after seeing their browsing history. Cookies and temporary files may affect a user's privacy since they disclose their online habits, but it is possible to modify the web browser preferences and limit their use. (Also see Tracking Cookie."

<b>TERM</b>	<b>DEFINITION</b>
<b><i>CoreBOT</i></b>	A modular Trojan from the infostealer category. CoreBOT was initially designed to collect and loot information from the infected computer or network. In time, CoreBOT quickly evolved and added other capabilities, such as browser-based web injects, real-time form-grabbing, man-in-the-middle attacks, etc. Now, its structure and tactics are similar to infamous financial malware strains, such as Dyreza or Neverquest. Its modular character makes CoreBOT appealing to cyber criminals because they can pack it with other types of malware and use it in complex cyber attacks.
<b><i>Covered information</i></b>	Information that KRGC has obtained from an entity (e.g., a licensee) in the process of offering a financial product or service (such as granting a license or certificate), or such information provided to the agency by another financial institution (such as the IRS). Examples include the applicant's addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.
<b><i>Credential</i></b>	An object that authoritatively binds an identity to a token possessed and controlled by a person or entity.
<b><i>Credential service provider, CSP</i></b>	A trusted entity that issues or registers tokens and issues electronic credentials.
<b><i>Critical system</i></b>	Any information system for which the loss, misuse, disclosure, unauthorized access to, or modification of information would result in a significant negative impact on the KRGC's core mission.
<b><i>Criticality</i></b>	The degree to which one depends on the information or information system for the success of a mission or of a business function.
<b><i>Crimeware</i></b>	Distinct from adware or spyware and is created for identity theft operations that use social engineering schemes to gain access to a user's online accounts. Crimeware is a growing issue for networks' security, as numerous types of malware look to steal valuable data from the systems. The retrieved information may be sent to other interested parties for a certain price.

TERM	DEFINITION
<b><i>Cross site scripting, XSS</i></b>	A software vulnerability usually found in web applications. XSS allows online criminals to inject client-side script into pages that other users view. The cross-site scripting vulnerability can be employed at the same time by attackers to over-write access controls. This issue can become a significant security risk if the network administrator or website owner does not take necessary security measures.
<b><i>Cyber attack</i></b>	Any type of offensive action used by an individual or organized group that targets computer networks, information systems, or large IT infrastructure by using various means to deploy malicious code for the purpose of stealing, altering, or taking advantage of this type of action. A cyber attack can appear under different names, including cyber campaign, cyber warfare, cyber terrorism, or online attack.
<b><i>Cyber incident</i></b>	When there is a violation of a security policy conducted on computer networks and the direct results affect an entire information system.
<b><i>Cybersecurity or cyber security</i></b>	A generalized term for organizing a defensive security strategy against online criminals and their malicious actions. A complete cyber security strategy includes multiple tools and methods to protect an operating system, network, computer, programs and data from attack, damage or unauthorized access by classic viruses, Trojans, spyware, and financial and data stealing malware. Cybersecurity strategy includes protection by use of VPN (virtual private network) software and backup solutions.  Also, security of data in any form which can be transmitted, received, stored, or cataloged, by electronic means. In the case of Protected Health Information (PHI), it would be health-related information in any form or medium.
<b><i>Cyber weapon</i></b>	An advanced and sophisticated piece of code that can be employed for military or intelligence purposes. The term has recently emerged from the military industry to name malicious software that can be used to access enemy computer networks.

**TERM****DEFINITION*****Cryptographic***

Related to cryptography, which is: (i) the mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key; (ii) a discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized uses.

***Cryptographic keys***

Data used to encrypt or decrypt a message or information.

***CryptoLocker***

CryptoLocker is a type of ransomware which emerged in 2013 and whose objective is to infect victims using PCs with Microsoft Windows. The primary distribution method is spam emails with a malicious attachment. CryptoLocker relies on external infrastructure (a botnet) to launch its attacks and, when activated, encrypts the files and data stored on the local device, but also those in cloud storage accounts, if, for example, a Dropbox account is synced locally on the affected PC. CryptoLocker then displays a message to demand victims pay a ransom (often in bitcoins) to receive the decryption key, which is stored on servers controlled by the cyber criminals.

***CryptoWall***

A ransomware Trojan which emerged as a CryptoLocker variant. CryptoWall spreads mainly through phishing and spam campaigns that invite users to click a malicious link or download and execute an email attachment. In order to increase distribution, cyber criminals often include CryptoWall code in website ads. The ransomware, once executed, encrypts all the data on the victim's PC and any other PC tied to the first affected computer by the same network. The victim is then prompted to pay a ransom in bitcoins in order to receive the decryption key and regain access to their data. CryptoWall has reached its fourth iteration and will likely continue to evolve.

***Curve-Tor-Bitcoin  
Locker virus, CTB  
Locker virus***

A dangerous malware and crypto virus found in the ransomware category of computer infections, similar to the FBI virus. Most versions of the CTB Locker virus use tactics to lock a computer system or internet browser and will claim to have encrypted a computer's files, in order to scare victims into paying a fine or ransom using bitcoin or other online services.

**TERM****DEFINITION**

***Cybersecurity Incident Response Team, C-SIRT***

The assigned individuals in the KRGC who investigate cybersecurity incidents. The team’s job is to analyze how the incident took place, what (if any) information was lost, and to provide a response.

***Cybersecurity Incident***

A violation or imminent threat of violation of computer security policies, acceptable uses, or standard computer security policies. Also includes any adverse event whereby some aspect of a computer system is compromised including loss of data confidentiality, disruption of data integrity, and disruption of availability which is also known as a denial of service.

***Cybersecurity Incident Response Team (C-SIRT):***

A group of staff members set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

**“D”**

***Damage***

The unauthorized deliberate or accidental physical or logical modification, destruction, or removal of information or data from an IT system.

***Dark web***

Refers to websites and online content that exists outside the reach of traditional search engines and browsers. This content is hidden by encryption methods (in most cases, these sites use the Tor encryption tool to hide their identity and location) and can only be accessed with specific software, configuration settings, or approval from their admins. The dark web is known for being a hub of illegal activities (drug and crime transactions, dark hat hacking, etc.)

***Data***

A subset of information in an electronic format that allows it to be retrieved or transmitted.

***Data asset***

A piece of information that contains valuable records. It can be a database, a document, or any type of information that is managed as a single entity. Like any asset, the information involved contains financial value that is directly connected to the number of people that have access to that data and should be protected accordingly.

***Data integrity***

Information property that has not been altered or modified by an unauthorized person. Refers to information quality in a database, data warehouse, or other online locations.

TERM	DEFINITION
<i>Data leakage</i>	A data loss of sensitive information, usually from a corporation or other large organization, that results in unauthorized personnel accessing valuable data assets. The sensitive data can be company information, financial details, or other forms of data that put the company name or its financial situation at risk.
<i>Data loss</i>	A process in which information is destroyed by failure or neglect during transmission or processing. Can sometimes occur because of cybercriminal action.
<i>Data theft</i>	Illegal operations in which private information is retrieved from an organization or an individual. The stolen data often includes credentials for online accounts and banking sites, credit card details, or valuable corporate information.
<i>Deep web</i>	Similar to the dark web, but is less criminal in nature. The world wide web content that has not been indexed by traditional search engines is known as the deep web and is preferred by certain groups for its increased privacy levels. Unlike the dark web, the deep web does not require its users to be particularly tech-savvy and is not hidden by sophisticated methods. A user only needs to know the address of the website to access it.
<i>Delegated administrator</i>	An administrator account, either a participating organization Delegated Administrator or an Entitlement Administrator.
<i>Denial-of-service attack, DoS</i>	A system attack that causes system resources to become unavailable. Examples include when an attacker has disabled a system, a network worm has saturated network bandwidth, an IP address has been flooded with external messages, or the system manager and all other users get locked out of a system.
<i>Distributed-denial-of-service attack, DDoS</i>	A type of online attack that is used to prevent normal users from accessing an online location. A cybercriminal can prevent legitimate users from accessing a website by targeting its network resources and flooding the website with a huge number of information requests.
<i>Deprecated technologies</i>	An element or attribute of technology that is being phased out and will no longer be supported or any elements or attributes that are currently not supported. A list of deprecated technologies is provided by the World Wide Web Consortium at <a href="http://www.w3.org/TR/REC-html40/index/elements.html">http://www.w3.org/TR/REC-html40/index/elements.html</a> .

TERM	DEFINITION
<i>Deprovision</i>	The process of enforcing the removal of a resource or disallowing its use by a user. The act of retiring a user's identity and terminating their access to IT systems and services.
<i>Descriptive link, D link</i>	A link to a page that provides a description of the image.
<i>Destroy</i>	The highest level of sanitizing data, after clear and purging. It renders target data recovery infeasible by using state-of-the-art laboratory techniques and causes the media to be incapable of storing data.
<i>Dialer</i>	A spyware device or program that is used to maliciously redirect online communication. Such a software disconnects the legitimate phone connection and reconnects to a premium rate number, which results in an expensive phone bill received by the user. Typically, it installs itself on the user's system.
<i>Digital footprint, digital dossier</i>	The body of data that exists as a result of actions and communications online that can in some way be traced back to an individual.
<i>Digital footprint manager, DFM</i>	An approach to controlling the amount and types of electronic data existing about a particular individual that can in some way be traced back to them.
<i>Digital object</i>	Any discrete set of digital data that can be individually selected and manipulated. This can include shapes, pictures, string of numbers, or characters that appear on a display screen as well as less tangible software entities.
<i>Digital signatures</i>	The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation.
<i>Directory Services Administrator, DSA</i>	The primary contact for each Participating Organization.
<i>Disaster Recovery Plan, DRP</i>	A set of procedures that are meant to protect or limit potential loss of business IT infrastructure in case of an online attack or major hardware or software failure. A recovery plan should be developed during the business impact analysis process.
<i>Discretionary access controls</i>	Access Controls based on the need-to-know, defined by the Entitlement Delegated Administrator.

<b>TERM</b>	<b>DEFINITION</b>
<i>Disk mirroring</i>	Also known as RAID 1, this is a form of disk backup in which anything that is written to a disk is simultaneously written to a second disk. This creates fault tolerance in the critical storage systems. If a physical hardware failure occurs in a disk system, the data is not lost, as the other hard disk contains an exact copy of that data.
<i>Disk striping</i>	A popular alternative to disk mirroring, in which data is striped in blocks over multiple volumes (disks). In case of a failure, the failed disk is recreated with the help of checksum or other data present on other disks. Unlike disk mirroring, disk striping may not fully recover lost data. Typically used for large applications which have several hundred gigabytes or terabytes of disk storage. Disk striping is one of the best techniques to use and can be performed in different ways. Disk striping is fault intolerant without parity. An advantage of disk striping is higher performance, but the drawback is that it has low resilience. If one of the several disks crashes, all data could be lost unless a high-reliability array with hot swap capabilities is used.
<i>Document malware</i>	Document malware takes advantage of vulnerabilities in applications that allow users read or edit documents.
<i>Domain generation algorithm, DGA</i>	A computer program used by various malware families to generate a large number of domains by creating slightly different variations of a certain domain name. The generated domains are used to hide traffic transmitted between the infected machines/networks and the command and control servers. By doing this cyber criminals can cover their tracks and keep their anonymity from law enforcement and private cyber security organizations. DGA domains are heavily used to hide botnets and their attacks.
<i>Domain Name Server hijacking, DNS hijacking</i>	An online attack that overrides a computer's TCP/IP settings to direct communication to a malicious server controlled by cybercriminals.
<i>Domain Name System cache poisoning, DNS cache poisoning</i>	A method used by online criminals to launch online attacks. This method modifies the domain name system, which results in it returning an incorrect IP address. The purpose is to divert traffic to a malicious server, which is controlled by hackers.
<i>Domain Name Server, DNS</i>	The system that translates internet addresses to the numeric machine addresses that computers use.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Domain Name System, DNS</i></b>	A hierarchical and decentralized naming system for computers, services, or other resources connected to the internet or private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, DNS has been an essential component of the functionality of the internet since 1985. DNS also specifies the technical functionality of the database service that is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the Internet Protocol Suite.
<b><i>Domain shadowing</i></b>	A malicious tactic used by cyber criminals to build their infrastructure and launch attacks while remaining undetected. First, attackers steal and gather credentials for domain accounts. Using these stolen credentials, they log into the domain account and create subdomains which redirect traffic towards malicious servers, without the domain owner having any knowledge of this. Domain shadowing allows cyber attackers to bypass reputation-based filters and pass their malicious traffic as safe.
<b><i>Dormant code</i></b>	Modern, advanced malware often has modular structure, including multiple components. One of them is dormant code, which means that the malware needs specific triggers to execute the task it was created for. This type of behavior is coded into the malware so it can bypass signature-based detection in products such as traditional antivirus and anti-malware solutions. There is also another reason for using dormant code: since advanced malware, such as ransomware or financial malware, usually rely on external infrastructure to download components for infection, the malware can remain dormant and undetected if it cannot reach its Control and Command servers to execute further.
<b><i>Dridex</i></b>	A strain of financial malware that uses Microsoft Office macros to infect information systems. Dridex is engineered to collect and steal banking credentials and additional personal information and its fundamental objective is banking fraud.
<b><i>Drive-by attack</i></b>	The unintentional download of a virus or malicious software (malware) onto a system. A drive-by attack will usually take advantage of or exploit a browser, app, or operating system that is out of date and has a security flaw.

TERM	DEFINITION
<i>Drive-by download</i>	A program that is automatically downloaded to a computer without the user's consent or knowledge.
<i>Dropper or dropper file</i>	A malware installer that surreptitiously carries viruses, back doors, and other malicious software so they can be executed on the compromised machine. Droppers do not cause harm directly but can deliver a malware payload onto a target machine without detection.
<i>Drive-by spamming</i>	A variation of drive-by hacking in which the perpetrators gain access to a vulnerable wireless local area network (WLAN) and use that access to send huge volumes of spam.
<i>Dual-factor authentication, two-factor authentication, 2FA</i>	A type of multi-factor authentication. A method of confirming a user's claimed identity in which access is granted only after the user successfully presents two pieces of evidence (factors) to an authentication mechanism.
<i>Dumpster diving</i>	Dumpster diving is the illegal method of obtaining passwords and corporate directories by searching through discarded media.
<i>Dyreza, Dyre</i>	A banking Trojan (financial malware) that appeared in 2014, whose behavior is similar to the Zeus family, although there is no connection between Dyreza and Zeus. The malware hides in popular web browsers that millions of users employ to access the web and aims to retrieve sensitive financial information every time the victim connects to a banking website. Dyreza is capable of key-logging, circumventing SSL mechanisms and two-factor authentication, and is usually spread through phishing emails.

## “E”

<i>Electronic authentication, e-authentication</i>	The process of establishing confidence in user identities electronically presented to an information system.
<i>e-Government</i>	The use of computer technology to provide faster, more convenient, and better delivery of government services to customers by reducing paper processes and the need to go to government offices in person. Customers of e-Government services can include citizens, businesses, and other governments. Typically, these services are available over the internet on a government agency's website or a government webpage.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Eavesdropping attack</i></b>	An attack that aims to capture information transmitted over a network by other computers. The objective is to acquire sensitive information like passwords, session tokens, or any kind of confidential information.
<b><i>Electronic evidence</i></b>	Defined by the United States Department of Justice Electronic Crime Scene Investigation as the information and data of investigative value that is stored on or transmitted by an electronic device.
<b><i>Electronic record, e-record</i></b>	Information that evidences any act, transaction, occurrence, event, or other activity, produced or stored by electronic means and capable of being accurately reproduced in forms perceptible by human sensory capabilities.
<b><i>Electronic signature, e-signature</i></b>	An electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record. An Electronic signature is defined by the federal E-Sign law.
<b><i>Elements</i></b>	HTML tags that are hidden keywords within a webpage that define how the web browser must format and display the content.
<b><i>Email malware distribution</i></b>	Although outdated, some malware programs still use email attachments as a mean of spreading malware and infecting users' computers. This type of infection relies on the user double clicking on the attachment. A current method that uses email as a dispersion mechanism inserts links to malicious websites.
<b><i>Employee</i></b>	Any individual employed by the Kansas Racing and Gaming Commission.
<b><i>Encoder</i></b>	A device used to change a signal (such as a bitstream) or data into a code. The code may serve many purposes such as compressing information for transmission or storage, encrypting or adding redundancies, transmission or storage, encrypting or adding redundancies to the input code, or translating from one code to another. This is usually done by a programmed algorithm, especially if any part of the code is digital.
<b><i>Encoding</i></b>	The process of preparing content for sending to viewers. Audio and video is converted to a format that matches the chosen distribution technique and attributes, then compressed.

TERM	DEFINITION
<i>Encrypted network</i>	A network on which messages are encrypted using a special algorithm in order to prevent unauthorized people from reading them.
<i>Encryption</i>	A technique used to protect the confidentiality of information. The process transforms (encrypts) readable information into unintelligible text through an algorithm and associated cryptographic key(s).
<i>End user</i>	Individuals using the services on the KRGC system which include employees, contractors, or other agents acting on behalf of the state or carrying out state agency functions.
<i>End-to-end encryption</i>	This process involves using communications encryption to make information unavailable to third parties. When being passed through a network, the information will only be available to the sender and the receiver, preventing ISPs or application service providers to discover or tamper with the content of the communication.
<i>End-to-end security</i>	The way of ensuring that data transmitted through an information system stays secure and safe from origin point to destination.
<i>Enterprise</i>	All state government. In some instances, enterprise expands beyond the state to include federal and local government partners in an effort to leverage resources across jurisdictions and expand information sharing capabilities.
<i>Enterprise Architecture, EA</i>	<p>Enterprise Architecture is a top-down, business strategic-driven process that coordinates the parallel, internally consistent development of enterprise business, information, and technology architectures, as well as the enterprise application portfolio. It represents the encompassing expression of the enterprise's key program, information, application, and technology strategies and their impact on program functions and processes. Conducted within an appropriate, collaborative organization/governance context, EA artifacts consist of common requirement vision and conceptual architecture, as well as current and future state models of four key components:</p> <ul style="list-style-type: none"> <li>• Enterprise Business Architecture (EBA);</li> <li>• Enterprise Information Architecture (EIA);</li> <li>• Enterprise Technical Architecture (ETA);</li> <li>• Enterprise Application Portfolio (EAP).</li> </ul>

TERM	DEFINITION
<b><i>Enterprise Application Portfolio, EAP</i></b>	A collection of integrated application systems required to satisfy program information needs, including the existing and planned inventory of applications and components, complete with relationships to supported information and business processes, and engineered linkages to the enterprise technical architecture and infrastructure services.
<b><i>Enterprise Business Architecture, EBA</i></b>	A business vision-driven, disciplined process that decomposes the enterprise's program strategies, the assets and processes required to execute them, as well as their impact on program functions.
<b><i>Enterprise Information Architecture, EIA</i></b>	A business-driven process that details the enterprise's information strategies, its extended information value chain, and the impact on technical architecture. The EIA delineates the key information artifacts of business events, models, and information flows, provides logically consistent information management principles, and enables rapid business decision making and information sharing.
<b><i>Enterprise Risk Management</i></b>	The methods and processes that organizations use to identify and manage cybersecurity risks that could endanger its corporate mission. As part of this plan, the organization will also establish a plan to protect its assets and a plan to react in case a cybersecurity risk becomes reality.
<b><i>Enterprise Technical Architecture, ETA</i></b>	An Enterprise Business Architecture and/or Enterprise Information Architecture driven, structured process that details the enterprise's technology strategies, its extended technology linkages, and their impact on program/project initiatives.
<b><i>Entitlement administrator</i></b>	An administrator account which is able to grant and remove KRGC application entitlements to user accounts, potentially across POs.
<b><i>Entropy</i></b>	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret such as a password. Entropy is usually stated in bits.
<b><i>Ethernet</i></b>	A system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.

<b>TERM</b>	<b>DEFINITION</b>
<i>Event</i>	Any observable or measurable occurrence in a system or network. Events may include, but are not limited to, a user connecting to a file share, a server receiving a request for a webpage, a user sending email, and the firewall blocking a connection attempt.
<i>Event handler</i>	Triggers which are fired when certain keyboard or mouse activity is detected such as clicked, focus, etc.
<i>Tabletop Exercises</i>	A scenario-driven simulation of an emergency, such as a power failure in one of the KRGC data centers or a natural disaster causing a full outage with additional situations often being presented during the course of an exercise, designed to validate the viability of one or more aspects of an IT plan. In an exercise, personnel with roles and responsibilities in a particular IT plan meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not involve using the actual operational environment.
<i>Executive branch agency</i>	K.S.A. 75-7237(g) defines as any agency in the executive branch of the state of Kansas, which does not include elected office agencies, the adjutant general's department, the Kansas public employee's retirement system, regents' institutions, or the board of regents.
<i>Exercise briefing</i>	Material and information that is presented to participants before and during an exercise to outline the exercise's agenda, objectives, scenario, and other relevant information.
<i>Exercise Director</i>	A person responsible for all aspects of an exercise, including staffing, development, conduct, and logistics.
<i>Existing system</i>	A commercial or homegrown system which is deployed prior to the effective date of a standard, and includes, without limitation, hardware, software, development tools, applications, and protocols.
<i>Explicit indication</i>	A signal or alert to user(s) physically present providing notice that a collaborative computing device sensor has been activated.

**TERM****DEFINITION**

<i>Exploit</i>	A piece of software, a chunk of data, or a sequence of commands that take advantage of a bug, a glitch, or a vulnerability in software in order to penetrate a user's system with malicious intent. The goal may include gaining control of a computer system, allowing privilege escalation, or launching a DoS attack.
<i>Exploit kit, EK</i>	Computer programs designed to find flaws, weaknesses, or mistakes in software apps (commonly known as vulnerabilities) and use them to gain access into a system or a network. They are used in the first stages of a cyber attack, because they have the ability to download malicious files and feed the attacked system with malicious code after infiltrating it.
<i>Exploit kits-as-a-service</i>	Exploit kits as-a-service is a relatively recent business model employed by cyber criminals in which they create, manage, sell, and/or rent exploit kits which are accessible and easy to use in cyber attacks. These exploit kits-as-a-service do not require much technical expertise to be used, are cheaper (especially if rented), are flexible, can be packed with different types of malware, offer broader reach, are usually difficult to detect, and can be used to exploit a wide range of vulnerabilities. This business model makes it very profitable for exploit kit makers to sell their malicious code to make money.
<i>External security testing</i>	Security testing conducted from outside the organization's security perimeter.
<i>Externally accessible to public</i>	Exists when a system can be accessed via the internet by persons outside of the agency without a logon id or password. The system may be accessed via dial-up connection without providing a logon id or password. It is possible to ping the system from the internet. The system may or may not be behind a firewall. A public web server is an example of this type of system.
<i>Extranet</i>	An intranet that is available to an authorized user outside the formal boundaries of the organization.

**"F"**

<i>Facilitator</i>	A person that leads a discussion among exercise participants.
--------------------	---

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Facilitator guide</i></b>	A document for an exercise facilitator that includes the material the facilitator needs for the exercise, such as the exercise's purpose, scope, objectives, and scenario; a list of questions regarding the scenario that address the exercise's objectives; and a copy of the IT plan being exercised.
<b><i>Fail-safe</i></b>	An automatic protection system that intervenes when a hardware or software failure is detected.
<b><i>Fake antivirus malware</i></b>	Rogue antivirus or rogue security is a form of computer malware that simulates a system infection that must be removed. The victims are asked for money in return for removal of the malware, but the removal program is nothing but a form of ransomware.
<b><i>False positive</i></b>	Occurs when a security solution detects a potential cyber threat which is a harmless piece of software or a benign software behavior.
<b><i>Federated architecture</i></b>	The structured expression of the state's key business, information, application, and technology strategies and their resulting impact on business functions and processes. To be successful in the development of a Technical Architecture, an organization must understand and account for the larger Federated Architecture context. Federated Architecture typically consists of current and future state models of four key components: Enterprise Business Architecture (EBA), Enterprise Information Architecture (EIA), Enterprise Application Portfolio (EAP), and Enterprise Technical Architecture (ETA).
<b><i>File binder</i></b>	Applications used by online criminals to connect multiple files together in one executable to launch malware attacks.
<b><i>File Transfer Protocol, FTP</i></b>	A protocol for transmitting files between computers on the internet. FTP is a client-server protocol where a client will ask for a file, and a local or remote server will provide it. The end-user's machine is typically called the local host machine, which is connected via the internet to the remote host—which is the second machine running the FTP software. It allows larger files to be transferred which email cannot. Similar to email this method is not encrypted.

TERM	DEFINITION
<i>Fileless malware</i>	Types of malicious code used in cyber attacks that do not use files to launch the attack or carry out the infection on the affected device or network. The infection is run in the RAM memory of the device, so traditional antivirus and antimalware solutions cannot detect it. Hackers use fileless malware to achieve stealth, privilege escalation, to gather sensitive information, and achieve persistence in the system so that the malware infection can continue to affect the device for a longer period of time.
<i>Financial malware</i>	A category of specialized malware designed to harvest financial information and use it to extract money from victims' accounts. Because it is a rather new type of malware, it is also very sophisticated and it can easily bypass traditional security measures, such as antivirus programs. Financial malware is capable of persisting in the affected system for a long time, until it gathers the information associated with financial transactions and to start leaking money from the targeted account.
<i>Finding</i>	A determination that an event or occurrence may cause a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.
<i>Firewall</i>	A specialized device or software program that controls the flow of network traffic between networks or hosts to enforce security policies and provide protection for the resources on those networks or hosts. Firewalls can protect networks and systems from exploitation of inherent vulnerabilities. Firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet.
<i>Flip button</i>	Appears when spyware or adware solutions trick users into following various actions and installing malicious software on the system.
<i>Flooding</i>	A security attack used by hackers against a number of servers or web locations. Flooding is the process of sending a large amount of information to such a location in order to block its processing power and stop its proper operation.
<i>Forensic specialist</i>	A professional who identifies and analyzes online traffic and data transfer in order to reach a conclusion based on the discovered information.

**TERM****DEFINITION*****Form-grabbing malware***

This type of malware can harvest confidential data when a user is filling a web form before the data is sent over the internet to a secure server. By doing this, the malware can avoid the security ensured by an HTTPS connection. Unfortunately, using a virtual keyboard, autofill, or copy/paste won't protect the data from this threat. The malware can categorize data according to type (username, password, etc.) and can grab the URL where the user was inputting their information.

***Frames***

A web browser feature that enables a web page to be displayed in an individual, independently scrollable window on a screen.

***Functional text***

Text that when read conveys an accurate message as to what is being displayed by the script.

***Fundamental alteration***

A major change or modification of the critical function or nature of a program or service.

**“G”*****Government Emergency Telecommunications Service, GETS***

During emergencies, the public telephone network can experience congestion due to increased call volumes and/or damage to network facilities, hindering the ability of first responders, national security, and emergency preparedness and response personnel to complete calls. GETS provides these essential personnel priority access and prioritized processing in the local and long-distance segments of the landline networks, greatly increasing the probability of call completion. GETS is intended to be used in an emergency or crisis situation when the network is congested and the probability of completing a normal call is reduced. GETS and WPS (wireless priority service) shall not be used at any other time other than for emergencies or crisis situations in which network systems are congested, or when tests are authorized by the IT-Cybersecurity unit and the GETS POC.

***GETS Point-of-Contact, GETS POC***

Every agency with GETS authority has a communications officer assigned as the point-of-contact. The GETS POC at the KRGC is the director of IT and Cybersecurity. This individual will authorize any test, ensure billings are complete and appropriate, and ensure annual renewals.

**TERM****DEFINITION**

***Gramm-Leach-Bliley Act***

Passed in 1999 and included provisions that limit the ability of financial institutions to disclose "non-public personal information" about consumers to non-affiliated third parties. This act requires financial institutions to provide customers with their privacy policies and practices with respect to non-public personal information.

***Greyhat hacker***

Operate more ambiguously compared to Blackhat and Whitehat hackers. For example, they may use illegal means to detect a vulnerability, but then will disclose it to the affected organization. Some search for exploits then sell their information to governments. Greyhat hackers are distinguished from Blackhat hackers because they do not use or sell the exploit for criminal gain.

***Guideline***

Non-mandatory suggested course of action.

**“H”**

***Health Insurance Portability and Accountability Act, HIPAA***

HIPAA is a federal act that sets a national standard for protecting the security and integrity of medical records when they are kept in electronic form.

***HTTPS scanning***

Another name for a Man-in-the-Middle attack. Scanning HTTPS (Hypertext Transfer Protocol Secure) content allows the attackers to decrypt, analyze, and re-encrypt content between websites that use SSL for security and a user's browser. This type of attack is usually used to snoop on information exchanges and to steal confidential data.

***Hacker***

A person who manages to gain unauthorized access to a computer system. There are three types of hackers: Blackhat hackers, Whitehat hackers, and Greyhat hackers.

***Hacktivism***

The activity of using hacking techniques to protest against or fight for political and social objectives. One of the most well-known hacktivist groups is Anonymous.

***Hashing***

The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. The numeric value changes if the information is modified which makes any modifications obvious.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Heartbleed vulnerability</i></b>	A security bug that appeared in 2014, which exposed information that was usually protected by SSL/TLS encryption. Because of a serious vulnerability that affected the OpenSSL library, attackers could steal data that was kept confidential by a type of encryption used to secure the internet. This bug caused around 500,000 web servers (17% of all servers on the internet) to be exposed to potential data theft.
<b><i>Hoax</i></b>	A false computer virus warning. A user may receive such hoaxes via email, instant messaging, or social media. Before acting on it, one should research online to check the validity of the claim. When a user has proof that the virus warning is fake, it is recommended to also inform the sender. Hoaxes can lead to malicious websites which can infect devices with malware.
<b><i>Homegrown system</i></b>	An automated non-commercial system which a state government entity develops or has developed for its own and/or another state government entity's use.
<b><i>Honeymonkey, Honey Client</i></b>	An automated system designed to simulate the actions of a user who is browsing websites on the internet. The purpose of the system is to identify malicious websites that try to exploit vulnerabilities that the browser might have.
<b><i>Honeypot</i></b>	A program used for security purposes which is able to simulate one or more network services that look like a computer's ports. When an attacker tries to infiltrate, the honeypot will make the target system appear vulnerable. In the background, it will log access attempts to the ports, which can even include data like the attacker's keystrokes. The data collected by a honeypot can then be used to anticipate incoming attacks and improve security in companies.
<b><i>Hot site</i></b>	A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption. Backup site that includes phone systems with the phone lines already connected. Networks will also be in place, with any necessary routers and switches plugged in and turned on. Desks will have desktop PCs installed and waiting and server areas will be replete with the necessary hardware to support business-critical functions. Within a few hours, a hot site can become a fully functioning element of an organization.
<b><i>Hot swap</i></b>	Ability to switch out components without powering down the unit, or having concern for a power surge.

**TERM****DEFINITION**

<i>Hot wash</i>	A debrief conducted immediately after an exercise or test with the staff and participants.
<i>Hub</i>	A networking device that allows one to connect multiple PCs to a single network. It differs from a switch in multiple ways, for example, a switch will have more ports. A hub is passive because it just connects the units and does not have software to operate. By contrast, a switch is an active intelligent device and requires software to function. A hub is slower than a switch and not as sophisticated.
<i>Hybrid attack</i>	Enhances a dictionary attack (used to crack passwords) by adding numerals and symbols so that credentials can be hacked even faster.
<i>Hypertext Markup Language, HTML</i>	A standardized system for tagging text files to achieve font, color, graphic, and hyperlink effects on World Wide Web pages.

**“I”**

<i>Intrusion Detection and Prevention System (IDPS):</i>	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.
<i>Identification method</i>	The technique used to obtain information regarding the user’s identity. Typically done as part of user account creation or promotion.
<i>Identity Assurance Level, IAL</i>	The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued and the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
<i>Identity theft</i>	The process of stealing someone’s personal identification data and using it online in order to pose as that person. Hackers can use a person’s name, photos, papers, social security number and so on, to gain financial advantage at this person’s expense (by obtaining credit or by blackmailing) or as a means of damaging the person’s reputation.
<i>Impact</i>	The magnitude of harm that could be caused by a threat or vulnerability.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Inadvertent disclosure</i></b>	This type of security incident involves accidentally exposing information to an individual who does not otherwise have access to that particular data.
<b><i>Incident / Cybersecurity incident</i></b>	A violation or imminent threat of violation of computer security policies, acceptable use, or standard computer security practices, conducted on computer networks and the direct results affect an entire information system. Includes any adverse event whereby some aspect of a computer system is compromised, such as loss of data confidentiality, disruption of data integrity, disruption, or denial of service. The types of incidents are classified into LOW, MEDIUM or HIGH levels depending on the severity. When there is a violation of a security policy conducted on computer networks and the direct results affect an entire information system
<b><i>Incident closure or closeout</i></b>	The last phase of incident handling lifecycle.
<b><i>Incident Declaration Independently Verified</i></b>	The phase of the incident handling lifecycle during which a state of Kansas incident number is assigned and the responsible state agency begins its incident handling process. An incident can be declared by a state of Kansas agency, staff, office, or the Cyber-Security Incident Response Team (C-SIRT), who is responsible for incident handling. Information provided by a user is verified by a source that is independent of the user (most often a trusted database) that the claimed identity exists and is consistent with the identity and address information provided. An independently verified destination is where credentials and tokens are issued or renewed in a manner that binds the verified user with an independently verified postal address of record of the user (e.g. by mailing an authenticator to the address of record) or telephone number of the user (e.g. by requiring a call from or to the applicant's telephone number of record).
<b><i>Incident handling</i></b>	The comprehensive management process of receiving incident indications and warnings from Intrusion Detection Systems (IDS), United States Computer Emergency Response Team, law enforcement or ISPs that an incident has occurred. Includes identifying the actual incident type, verifying the victim or perpetrator's responsible agency, and alerting the agency. Incident handling also requires reporting, responding to, mitigating, and closing a state of Kansas cybersecurity incident.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Incident log</i></b>	The process and requirement for state of Kansas and its agencies to maintain comprehensive records of all incidents from the time of declaration through closure. The state and its agencies are required to track incidents and report the status of those incidents periodically to the Enterprise Security Officer, and the Kansas IT Security Council. The agency is required to log the manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.
<b><i>Incident notification</i></b>	This phase of the incident handling lifecycle involves the formal transmission of declared incident information to the documented incident handling or management personnel in the Kansas agency that is experiencing a cybersecurity incident.
<b><i>Incident oversight</i></b>	The process of ongoing review and follow-up of incident status by the state of Kansas IT Enterprise Security Office, staff, or assignees to maintain accurate incident records on the number of incidents declared open, closed or cancelled. Statewide incident oversight is required for record keeping and review of closeout reports.
<b><i>Incident preparation</i></b>	This phase of the incident handling lifecycle involves preparing reports and providing continuous status on the incident.
<b><i>Incident prevention</i></b>	This phase of the incident handling lifecycle involves the review of alerts, warnings, and suspected events from various sources. Incident prevention requires continuous system monitoring and review of risk assessments for systems with high cybersecurity incident rates.
<b><i>Incident reporting</i></b>	This phase involves a formal acknowledgement by the incident handler that a cybersecurity incident has occurred and that all personnel responsible for responding to, acting upon, or resolving an incident have been notified.
<b><i>Incident response, IR</i></b>	The process of acting upon identified incidents. The process includes a forensic analysis of how the incident occurred, actions to contain the incident, eradicate the cause of the incident, repair the damage, and recover from the incident. Includes collection and preparation of a lessons learned report and assistance in the development of an incident report.
<b><i>Incident response stakeholders</i></b>	Any individuals (technical or non-technical) who directly respond to or oversee IR activities.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Incremental backups</i></b>	A type of backup that will only back up the files that have been modified since performing the last backup. Incremental backups are faster and ensure that data is always backed up.
<b><i>Independently verified</i></b>	Describes information provided by a user that is verified by a source independent of the user (most often a trusted database). The independent source confirms that the claimed identity exists and is consistent with the identity and address information provided.
<b><i>Independently verified destination</i></b>	An independently verified destination is where credentials and tokens are issued or renewed in a manner that binds the verified user with an independently verified postal address of record of the user (for example, by mailing an authenticator to the address of record); telephone number of the user (for example, by requiring a call from or to the applicant's telephone number of record).
<b><i>Information</i></b>	Any representation of facts, concepts, or instructions that are created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. This may include, but is not limited to, data contained in reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic, or hard copy.
<b><i>Information asset</i></b>	A body of information defined and managed as a single unit, so it can be understood, shared, protected and exploited effectively.
<b><i>Information assurance, IA</i></b>	A set of measures designed to protect and defend data and information systems by ensuring that their availability, integrity, confidentiality, and authenticity. These measures include having a data backup to restore information in case of data loss, having cybersecurity safeguards in place, and ensuring that detection and reaction capabilities are present.
<b><i>Information classification</i></b>	The process of identifying information assets, then classifying those assets by confidentiality, integrity, and availability (CIA) and determining controls based upon the classification. (See KRGC Cybersecurity Policy 2020-06 Information Classification for additional information.)
<b><i>Information flow control</i></b>	An important safeguard that ensures that data transfers in an information system comply with the security policy and are as secure as possible.

<b>TERM</b>	<b>DEFINITION</b>
<i>Information maturity</i>	The relative ability or inability of an organization to ensure data is high-quality, accurate, available and utilized by the jurisdiction to make informed program decisions.
<i>Information owner</i>	An individual or organizational unit responsible for making classification and control decisions regarding use of information.
<i>Information security</i>	The concepts, tactics, tools, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure, or temporary or permanent loss. Its purpose is to ensure the confidentiality, integrity, and availability of the data and information systems.
<i>Information Security Administrator</i>	An employee of IT shall be designated as the Security Administrator for the agency.
<i>Information security policy</i>	A set of guidelines, directives, regulations, rules, and practices that define how an organization will manage, protect and distribute information.
<i>Information security risk</i>	A risk that is evaluated according to how and how much it threatens an organization's operations (including mission, functions, brand, reputation) or assets, employees, partners etc. A risk is based on the potential for cyber criminals to gain unauthorized access and use it to collect confidential data, disclose it to the public or to unauthorized parties, modify it or destroy it, thus disrupting the organization's activity.
<i>Information Security Officer</i>	An individual in the Information Technology and Cybersecurity Unit who reports directly to the Director of Information Security and Cybersecurity and is part of the C-SIRT.
<i>Information security program</i>	The administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered information. Includes any peripheral parts such as training and monitoring.
<i>Information system</i>	A discrete set of information system components organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. Information systems also include specialized systems such as industrial/process control systems, telephone switching, private branch exchange systems, and environmental control systems.

TERM	DEFINITION
<i>Information system component</i>	ITEC 7230 §5.4: a discrete, identifiable information technology asset such as hardware, software, firmware, or media (electronic and hardcopy) that represents a building block of an information system. Information system components include commercial information technology products.
<i>Information system resilience</i>	A system that can continue to work even while under attack, even if it becomes degraded or weakened. A resilient system is able to quickly recover from a successful attack and regain operational capabilities, at least for core functions.
<i>Information Security, INFOSEC</i>	The protection of information systems against unauthorized access or attempts to compromise and modify data, whether it's stored data, processed data, or transmitted data. Includes the necessary measures to detect, document, and counter these threats.
<i>Information technology resources</i>	Equipment or services used to input, store, process, transmit, and output information, including but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, internet, email, and social media sites.
<i>Inside threat</i>	Refers to employees or other people with authorized access who can potentially harm an information system by destroying all or parts of it, by disclosing or modifying confidential information, and/or by causing denial of service.
<i>Integrity</i>	The characterization that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.
<i>Intellectual property</i>	Useful artistic, technical or industrial information, concepts, ideas or knowledge that clearly show that they are owned by someone who has control over them, either in physical form or in representation.
<i>Internal security testing</i>	Testing that is conducted from inside an organization to examine the resilience and strength of an organization's security perimeter and defenses.
<i>Internet</i>	A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
<i>Internet Protocol Address, IP Address</i>	A numerical identifier assigned either to a user's internet service provider or directly to a user's computer.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Internet worm</i></b>	Created by researchers in the 1980s to find a reliable way of growing the internet through self-replicating programs that can distribute themselves automatically through the network. An internet worm distributes itself across the web by using the computers' internet connection to reproduce.
<b><i>Intranet</i></b>	A network belonging to an organization, available only to the organization's members, employees, or others with authorization.
<b><i>Intruder</i></b>	A person who is the perpetrator of a computer security incident. Intruders are often referred to as "hackers" or "crackers." Hackers are highly technical experts who penetrated computer systems; the term crackers refers to the experts with the ability to "crack" computer systems and security barriers. Most of the time "cracker" is used to refer to more notorious intruders and computer criminals. An intruder is a vandal who may be operating from within the KANWIN network or attacking from the outside.
<b><i>Intrusion</i></b>	An unauthorized, inappropriate, or illegal activity by insiders or outsiders that can be considered a penetration of a system. This is usually by circumventing a system's security mechanisms to gain unauthorized access.
<b><i>Intrusion detection systems, IDS</i></b>	A security management system set up to actively protect computer and networks. It works by analyzing information from various areas of a computer/network to spot potential security breaches. These breaches can be either caused by intrusions (external attacks) and misuse (insider attacks). IDS monitors the packet flow, not the files.
<b><i>IP flood</i></b>	A DoS attack which aims to send a host an avalanche of pings (echo request packages) that the protocol implementation cannot manage. This causes a system to fail and send a DoS error.

**TERM****DEFINITION*****IP spoofing***

A tactic used by cyber criminals to supply a false IP address that masquerades as a legitimate IP. This helps the attacker gain an unfair advantage and trick the user or cybersecurity solution that is in place.

***ITEC***

Kansas Information Technology Executive Council. This group is responsible for adopting: information technology resource policies, procedures, and project management methodologies for all state agencies; an information technology architecture, including telecommunications systems, networks and equipment that covers all state agencies; standards for data management for all state agencies; and a strategic information technology management plan for the state. It provides direction and coordination for the application of the state's information technology resources, and designates the ownership of information resource processes and the lead agency for implementation of new technologies and networks shared by multiple agencies in different branches of state government.

**“J”*****Joint photographic experts group, JPEG, jpeg******Jamming***

An attack in which a device emits electromagnetic energy on a wireless network's frequency to make the network unusable. An attack that attempts to interfere with the reception of broadcast communications. (This occurs on radios when two radios are simultaneously transmitting on the same frequency.)

**“K”*****KISO***

The Kansas information security office.

***KRGC private, trusted network***

The network on KRGC property where only KRGC equipment is used, or under KRGC control, and a closed network where operators have integrity at each and every network connection.

***KRGC risk register, KRGC risk log***

A spread sheet, application, or database that the agency can use during risk assessments or risk identification. The risk register enables whoever conducts a risk assessment to log the threat, assets impacted, and threat probability.

**TERM****DEFINITION**

<b><i>KRGC user</i></b>	Any person authorized to access the KRGC network.
<b><i>KRGC user account</i></b>	An account in the KRGC network that is identified by a user ID. A KRGC user account may be authorized to perform specific functions within the KRGC.
<b><i>Key escrow</i></b>	A cryptographic key exchange process in which a key is held in escrow, or stored, by a third party. A key that is lost or compromised by its original user(s) may be used to decrypt encrypted material, allowing restoration of the original material to its unencrypted state.
<b><i>Keylogging</i></b>	Malware that can record the keystrokes on a user's keyboard, without the victim realizing it. This malware enables cyber criminals to collect information such as passwords, usernames, PIN codes, and other confidential data.
<b><i>Kovter</i></b>	Kovter is a Trojan whose primary objective is performing click-fraud operations on the PC it compromises. In 2015 Kovter incorporated new cloaking tricks in order to evade detection, which enabled cyber criminals to use it to deliver other types of malware, such as ransomware, or to recruit PCs into botnets.

**“L”**

<b><i>Local Area Network, LAN</i></b>	A computer network that links devices within a building or group of adjacent buildings.
<b><i>LAN Manager hash, LM hash</i></b>	A method of securely storing passwords in a system. Passwords are not stored in true-text, they are hashed then stored. LM hash is a compromised password hashing function that was the primary hash for Microsoft LAN Manager and Microsoft Windows versions prior to Windows NT. Newer versions will store both NTLM and LM if passwords less than 15 characters are used, making the system as vulnerable as pre-NTLM hashing for those using smaller passwords. (The simplest way to prevent Windows from storing an LM hash of a password is to use a password that is at least 15 characters long. By doing so, Windows stores an LM hash value that cannot be used to authenticate the user. This occurs because hashing function adds zeros to the longer digits, causing a different hash in LM, but NTLM remains consistent.)

<b>TERM</b>	<b>DEFINITION</b>
<i>Landing page, home page</i>	The webpage where a visitor lands when they have clicked on a Google AdWords ad or similar search result. It is any webpage that a user arrives at after clicking a hyperlink. The definition of landing page has changed from being synonymous with a website's home page to referring to any page within a website that is linked to from another location on the web.
<i>Least privilege</i>	Granting users, programs, or processes only the access they specifically need to perform their business task and no more.
<i>Level of Assurance, LoA</i>	The degree of confidence in the processes leading up to and including the authentication. The LoA provides assurance that the entity claiming a particular identity is the entity to which that identity was assigned. See Identity Assurance Level (IAL)
<i>Level of concern</i>	The rating which indicates which protection tactics and processes should be applied to an information system to keep it safe and operating at an optimum level. Levels of concern include basic, medium, or high.
<i>Level of consequence</i>	The impact an incident has on an organization. Impact includes loss of data, the cost to a Kansas agency or mission area, negative consequences to the organization (e.g. damage to reputation), and the magnitude of damage that must be repaired.
<i>Likelihood of occurrence</i>	The probability of specific threats to exploit a given vulnerability, based on a subjective analysis.
<i>Locky</i>	A type of encrypting malware and ransomware that is distributed through Microsoft Office Macros and targets Windows PCs. The name originates from the file extension it uses. Once a victim's PC is infected, the ransomware will scramble and encrypt all the data on that PC, setting every file extension to ".locky." Locky is spread through spam email campaigns, which make heavy use of spoofing. Locky creators demand a ransom in exchange for decrypting the data and if the ransom is not paid, the data will be left useless.
<i>Log management infrastructure</i>	The hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data.
<i>Logic bomb</i>	A piece of code that a malicious actor can insert into software to trigger a malicious function when a set of defined conditions are met.

**TERM****DEFINITION*****Low impact***

This level of impact of a cyber threat or cyber attack on an organization includes potential loss of confidentiality, integrity, or availability, but with limited consequences. Low impact incidents can reduce the capabilities of the organization, while still retaining the ability to function, and also cause other minor damages, financial loss, or harm to people.

**“M”*****Macro virus***

A type of virus that attaches itself to documents and uses macro programming options in a document application (such as Microsoft Word or Excel) to execute malicious code or propagate itself.

***Major upgrade***

Includes, but is not limited to, substantial redesign of an existing system for the purpose of providing new application functionality, upgrades to a new major version or releases of a proprietary software product, or application modifications which would involve substantial administrative or fiscal resources to implement.

***Malicious act***

An intentional act to attempt or cause harm or damage without justification.

***Malicious applet***

A small application that is automatically downloaded and execute and is capable of performing an unauthorized action/function on an information system.

***Malicious code***

A type of software camouflaged to seem useful and suitable for a task, but which actually obtains unauthorized access to system resources or fools a user into executing other malicious actions.

***Malware advertisement, malvertisement***

An online ad infected with malicious code that can be injected into a safe, legitimate website, without the website owner's knowledge.

***Malicious advertising, malvertising***

The process by which malware is distributed through online advertising networks. This technique is widely use to spread financial malware, data-stealing malware, ransomware, and other cyber threats.

***Malware***

A virus, worm, Trojan horse, or other code-based malicious software that successfully infects a host.

TERM	DEFINITION
<b><i>Malware-as-a-service</i></b>	A type of malware developed by cyber criminals to require little or no expertise in hacking, to be flexible, polymorphic, offer a broader reach and often comes packed with ready-coded targets. Malware-as-a-service can be bought or rented on the deep web and in cyber criminal communities and can sometimes include technical support from its makers and their team, which they run as a business.
<b><i>Man-in-the-middle attack, MITM, MITMA, or MIM</i></b>	A cyber attack in which cyber criminals can change the victim's web traffic and interpose themselves between the victim and a web-based service the victim is trying to reach. The attacker can then either harvest the information that is being transmitted via the web or alter it for their needs.
<b><i>Mandatory access controls</i></b>	A type of access controls which are enforced by the KRGC, based on the security level and allowable authentication methods of the KRGC application.
<b><i>Mandatory standard</i></b>	A standard which must be complied with by state government. Exemptions are not granted or considered from mandatory standards.
<b><i>Master scenario events list, MSEL</i></b>	A chronologically sequenced outline of the simulated events and key event descriptions that participants will be asked to respond to during an exercise.
<b><i>Maximum tolerable downtime</i></b>	The maximum amount of time that organizational processes and activities can be disrupted without causing severe consequences for the organization's mission.
<b><i>Mazar BOT</i></b>	A strain of malware targeting Android devices. The malware spreads through SMSs sent to random numbers, which include a link shortened through a URL shortener service (such as bit.ly). Once clicked, the link installs the Mazar BOT malware on the affected device, gaining the ability to write, send, receive, and read SMS, access internet connections, call phones, erase the phone it is installed on and many more. Mazar BOT does not run on smartphones running iOS, Apple's operating system.
<b><i>Message inject</i></b>	A pre-scripted message that will be given to participants during the course of an exercise.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Mobile code</i></b>	A type of software that can be transferred between systems (across a network) and which can also be executed on a local system, such as a computer, without the recipient's explicit consent. Some examples of mobile code include: JavaScript, VBScript, Flash animations, Shockwave movies, Java applets, ActiveX controls, and macros embedded in Microsoft Office or Excel documents.
<b><i>Mobile device</i></b>	A computing device is a portable small form factor that has at least one network connection interface, non-removable, and/or removable storage, including but not limited to smartphones, personal digital assistants (PDAs), tablets, laptops, smart watches, and other wearable devices.
<b><i>Mobile phone malware</i></b>	A type of malware specifically targeting mobile phones, tablets, and other mobile devices that aims to disrupt their normal functions, cause system damage, data leakage, and/or data loss.
<b><i>Moderate impact</i></b>	This type of impact is estimated or observed on an information system and involves a significant blow to a system's confidentiality, integrity, or availability. The organization may record barely working primary functions and significant damage to its assets, finances and individuals.
<b><i>Multi-factor authentication, multifactor authentication, or MFA</i></b>	<p>ITEC 7230 §5.5 defines as: a method of confirming a user's claimed identity in which access is granted only after successfully presenting two or more different pieces of evidence (factors) to an authentication mechanism. 2FA is a form of MFA that uses two factors. Factors include knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is). MFA uses more than one of these factors to authenticate to a system:</p> <ul style="list-style-type: none"> <li>• Something the user knows (e.g., user-ID, password, personal identification number (PIN), or passcode);</li> <li>• Something the user has (e.g., a one-time password authentication token, 'smart card');</li> <li>• Something the user is (e.g., fingerprint, retina scan).</li> </ul>
<b><i>Mung</i></b>	A backronym meaning "Mash Until No Good." According to <i>The New Hacker's Dictionary</i> , mung is (1) a verb, used in a derogatory sense, meaning to imperfectly transform information, or (2) a noun meaning a comprehensive rewrite of a routine, data structure, or the whole program.

**TERM****DEFINITION**

***Munge*** A backronym meaning “Modify Until Not Guessed Easily.” Munge is an attempt to create a strong, secure password through character substitution. The usage differs significantly from mung, because munging implies destruction of data, while mungeing implies creation of strong protection for data.

**“N”**

***National Institute of Standards and Technology, NIST***

The federal agency under the U.S. Department of Commerce that created and promulgated technology standards.

***NT-LAN Manager hash, NTLM hash***

A method of securely storing passwords in a system. Passwords are not stored in true-text, they are hashed then stored. LM hash is a compromised password hashing function that was the primary hash method for Microsoft LAN Manager and Microsoft Windows versions prior to Windows NT (New Technology). Newer versions store both NTLM and LM if passwords are less than 15 characters, making the system as vulnerable as pre-NTLM hashing for those using smaller passwords.

***Need-to-know***

The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. The responsibility for determining whether a person’s duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient.

***Negligence***

A failure to exercise the appropriate and/or ethical care expected under specified circumstances. Negligence involves harm caused by failing to act as a form of carelessness, possibly with extenuating circumstances. The core concept of negligence is that people should exercise reasonable care in their actions, by taking account of the potential harm that they might foreseeably cause to other people or property.

***Netiquette***

Short for network etiquette. Is a collection of best practices and things to avoid when using the internet, especially in communities such as forums or online groups. This is more of a set of social conventions that aim to make online interactions constructive, positive and useful. Examples include: posting off-topic, insulting people, sending or posting spam, etc.

<b>TERM</b>	<b>DEFINITION</b>
<i>Network owner</i>	An individual or organizational unit responsible for operating and maintaining the physical and virtual infrastructure which comprises the network, including responsibility for establishing the procedures to be used for maintenance and upgrades.
<i>Network packet</i>	See packets.
<i>Network sniffing</i>	A software program to monitor and analyze network traffic. This can be used legitimately, to detect problems and keep an efficient data flow. It can also be used maliciously to harvest data that is transmitted over a network.
<i>Network switch</i>	See switch.
<i>Network Time Protocol</i>	Networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
<i>Neutrino</i>	An exploit kit which has been constantly evolving since it appeared in 2013. This exploit kit rose to fame because of its user-friendly features and low entry barrier to using it. Neutrino includes a user-friendly control panel, continuous monitoring of antivirus detection rates, infostealer capabilities, recommendations of which exploits to use, and more. Neutrino is a tool often used to compromise PCs and deliver different types of malware. It is delivered through malvertising campaigns and web injects. Neutrino is also available through the exploit kit-as-a-service model, where attackers can rent the exploit kit and increase their profits with smaller investments.
<i>Node</i>	A node is any physical device within a network of other devices that is able to send, receive, and/or forward information. Modems, switches, hubs, bridges, servers, and printers are all nodes, as are other devices that connect over Wi-Fi or Ethernet. For example, a network connecting three computers and one printer, along with two other wireless devices, has six total nodes. Nodes within a computer network must have some form of identification, like an IP address or MAC address, for it to be recognized by other network devices. A node without this information, or one that has been taken offline, no longer functions as a node.
<i>Noframes</i>	A webpage displayed without frames.

**TERM****DEFINITION**

<i>Nonce</i>	A value used in security protocols that is never repeated with the same key. For example, Nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise there is a possibility of a replay attack. Using a Nonce as a challenge is a different requirement than a random challenge, because a Nonce is not necessarily unpredictable.
<i>Non-repudiation</i>	A system's ability to prove that a specific user (and that user alone) sent a message and that the message has not been modified.
<i>Nuclear Exploit Kit</i>	A highly effective exploit kit which appeared in 2010 and gave cyber criminals the opportunity to exploit a wide range of software vulnerabilities in applications such as Flash, Silverlight, PDF reader, Internet Explorer, and more. The kit is polymorphic in nature so it advanced over the years into a notorious tool used for launching zero-day attacks, spreading ransomware, or for data exfiltration operations. Nuclear Exploit Kit was often used in high-volume compromises and gave attackers the ability to customize their attacks to specific locations and computer configurations. This constantly evolving exploit kit features various obfuscation tactics in order to avoid being detected by traditional anti-virus and anti-malware solutions.

**“O”**

<i>Obfuscation</i>	A tactic used to make computer code obscure or unclear, so that humans or certain security programs (such as traditional antivirus software) cannot understand it. When using obfuscated code, cyber criminals make it difficult for cybersecurity specialists to read, analyze, and reverse engineer the malware thereby preventing specialists from determining a method to block the malware and suppress the threat.
<i>Offline attack</i>	A type of attack that occurs when an attacker manages to gain access to data through offline means (such as eavesdropping or looking over someone's shoulder to obtain their credentials) to penetrate a system and steal confidential information.
<i>Online service</i>	A service accessed via the internet or other networks which provides access to citizens, businesses, business partners, state entities, local government entities, and state employees.

**TERM****DEFINITION*****Operation Tovar***

An international, collaborative effort undertaken by law enforcement agencies and private security companies from multiple countries. The operation's main objective was to take down the Zeus GameOver botnet, which was believed to be distributing the CryptoLocker ransomware. Heimdal Security was involved in this effort alongside the U.S. Department of Justice, Europol, the FBI, Microsoft, Symantec, Sophos, Trend Micro, and others.

***Outside threat***

An unauthorized person from outside the organization's security perimeter who has the capacity to harm an information system by destroying it, modifying or stealing data from it, disclosing that data to unauthorized recipients, and/or causing denial of service.

**"p"*****Packet, network packet***

A formatted unit of data carried by a packet-switched network. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. When data is formatted into packets, the bandwidth of the communication medium can be better shared among users than if the network were circuit switched. Packets have an established structure, consisting of the header (containing information about the packet), the payload (containing the actual data being transmitted), and the trailer (advising the end of the packet or end-of-file).

***Packet sniffer***

A type of software designed to monitor and record traffic on a network. Can be used to run diagnostic tests and troubleshoot potential problems. Can also be used for malicious purposes, such as snooping on private data exchanges, including web browsing history, downloads, email recipients, etc.

***Parasitic viruses***

A type of virus that is capable of associating itself with a file or inserting itself into a file. To remain undetected, this virus will give control back to the software it infected. When the operating system looks at the infected software, it will continue to give it rights to run as usual. The virus will be able to copy itself, install itself into the computer's memory, or make other malicious changes to the infected computer. This type of virus was common in early computer history, waned in usage, but is becoming more common again.

<b>TERM</b>	<b>DEFINITION</b>
<i>Passive attack</i>	A type of attack during which cyber criminals try to gain unauthorized access to confidential information. Because the attacker only extracts information without changing the data it is more difficult to detect.
<i>Password</i>	Secret combination of keyboard characters consisting of a sequence of letters, numbers, special characters, or other text used to authenticate a user's identity.
<i>Password expiration</i>	A mandatory date or number of days when a password expires and must be changed by the user to continue to have access to the system.
<i>Password sniffing</i>	A tactic used by cyber criminals to harvest passwords. Achieved by monitoring and snooping on network traffic to retrieve password data. For example, if a password is sent over an unencrypted connection (e.g. by inputting a password on a website that is not protected by a security certificate), then it is easy for attackers to obtain that password.
<i>Patch</i>	A small software update released by manufacturers to fix or improve a software program. A patch can fix security vulnerabilities and bugs, or enhance the software's features, usability, and performance.
<i>Patch management</i>	The activity of getting, testing and installing software patches for a network and the systems in it. Patch management includes applying patches both for security purposes and for improving the software programs used in the network and the systems within it.
<i>Patching</i>	The act of applying a patch, which is designed to fix or enhance a software program. This includes both security-related updates and improvements in terms of software features and user experience.
<i>Patriot Act</i>	See U.S.A. Patriot Act.
<i>Payload</i>	The data cargo transported by a piece of malware onto the affected device or network. The payload contains the fundamental objective of the transmission, which is why the payload is actually the element of the malware that performs the malicious action (i.e. stealing financial information, destroying data, encrypting data on the affected device/network).

TERM	DEFINITION
<i>Penetration testing, pen testing</i>	A test of the overall strength of an SE's defenses (technology, processes, and people) by simulating the objectives and actions of an attacker.
<i>Persistent cookie</i>	A cookie that remains on the user's computer.
<i>Personal computer, PC</i>	A computer that is intended to be operated directly by an end user, rather than by a computer expert or technician.
<i>Personal financial information, PFI</i>	Any non-public personally identifiable financial information that an entity collects about an individual in order to provide a financial product or service.
<i>Personal information</i>	Any information concerning a natural person which, because of name, number, symbol, mark, or other identifier, can be used to identify that natural person.
<i>Personally identifiable information, PII</i>	Any information that can be used on its own or with other information to identify or locate a single person.

## TERM

## DEFINITION

### *Personal, private, or sensitive information, PPSI*

Any information where unauthorized access, disclosure, modification, destruction, or disruption of access to or use of such information could severely impact the agency's critical functions, its employees, its customers, or third parties. This term shall include, but is not limited to, the information encompassed in existing statutory definitions:

- Information concerning a person which, because of name, number, personal mark or other identifier, can be used to identify that person, in combination with:
- Social Security Number;
- Driver's license number or non-driver identification card number;
- Mother's maiden name (or any other personal family information); or financial account identifier(s) or other information which would permit access to a person's financial resources or credit.
- Information used to authenticate the identity of a person or process (e.g., PIN, password, passphrase, biometric data). This does not include distribution of one-time-use PINs, passwords, or passphrases.
- Information that identifies specific structural, operational, or technical information, such as maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities, including, but not limited to:
- Training and security procedures at sensitive facilities and locations as determined by the Office of Homeland Security (OHS); descriptions of technical processes and technical architecture plans for disaster recovery and business continuity; and reports, logs, surveys, or audits that contain sensitive information. Security related information (e.g., vulnerability reports, risk assessments, security logs).
- Other information that is protected from disclosure by law or relates to subjects and areas of concern as determined by executive staff.

### *Persons with disabilities*

A person with (1) a physical, mental, or medical impairment resulting from anatomical, physiological, genetic or neurological conditions which prevents the exercise of a normal bodily function or is demonstrable by medically accepted clinical or laboratory diagnostic techniques; (2) a record of such an impairment; or (3) a condition regarded by others as such an impairment.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Pharming</i></b>	May begin as a phishing incident and could have a link that looks legitimate. However, it will redirect internet traffic from a legitimate website to a fake one so that victims input their confidential information for attackers to collect. This type of attack typically targets banking and ecommerce websites. This can be difficult to detect because a victim can type in the correct URL but still be redirected to the fake website operated by cyber-criminals.
<b><i>Phishing</i></b>	A malicious technique used by cyber criminals to gather sensitive information (credit card data, usernames and passwords, etc.) from users. Attackers pretend to be a trustworthy entity to bait the victims into trusting them and revealing their confidential data. The data gathered through phishing can be used for financial theft, identity theft, to gain unauthorized access to the victim's accounts, or to blackmail the victim.
<b><i>Physical and environmental security controls</i></b>	<p>Measures taken to protect systems and physical infrastructure against threats associated with their physical environment. Physical and environmental security controls include the following broad areas:</p> <ul style="list-style-type: none"> <li>• The facility's general geographic operating location determines the characteristics of natural threats, such as earthquakes and flooding; man made threats such as burglary, civil disorders, or interception of transmissions and emanations; and damaging nearby activities, including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters, such as radars.</li> <li>• Supporting facilities are those services, both technical and human, that underpin the operation of the system. The system's operation usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the system and may cause physical damage to system hardware or stored data.</li> </ul>
<b><i>Physical infrastructure</i></b>	A generic description of any area containing non end-user IT equipment and subsidiary hardware, e.g. mainframes, servers, communications equipment, printing facilities, media libraries, and wiring closets.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Physically secured area</i></b>	<p>Area that is secured by an access control system that has the following components:</p> <ul style="list-style-type: none"> <li>• Requires dual factor authentication to access;</li> <li>• Designed to prevent abuse of the system, such as tailgating or rendering the system inoperable (by wedging doors open);</li> <li>• Keep a record of those who are allowed access;</li> <li>• Print a list of those allowed entry to the room;</li> <li>• Create a log of all those who enter the secure area;</li> </ul> <p>If the device relies on physical tokens (such as magnetic cards) it should be possible at any time to account for the location of all such tokens in order to have a fail-safe in the event of a system failure.</p>
<b><i>Plaintext</i></b>	<p>In cryptography, plaintext refers to any message that is not encrypted and therefore easily read and understood.</p>
<b><i>PO Delegated Administrator</i></b>	<p>An administrator account which is able to manage user accounts owned by a PO.</p>
<b><i>Policy</i></b>	<p>A prescribed or proscribed course of action or behavior which is to be followed with respect to the acquisition, deployment, implementation, or use of information technology resources.</p>
<b><i>Polymorphic code</i></b>	<p>Code that is capable of mutating and changing while maintaining the initial algorithm. Each time it runs, the code morphs, but keeps its function. This tactic is often used by malware creators to keep their attacks covert and undetected by reactive security solutions.</p>
<b><i>Polymorphic engine</i></b>	<p>A computer program that generates polymorphic malware. It is capable of transforming a program in derivative versions (different versions of code), but which perform the same function. Polymorphic engines rely on encryption and obfuscation to work, and are used almost exclusively by malware creators and other cyber criminals. Using this type of engine, malicious hackers can create malware types that cannot be detected by antivirus engines or have a very low detection rate.</p>
<b><i>Polymorphic malware</i></b>	<p>Polymorphic malware is capable of transforming itself into various derivative versions that perform the same function and have the same objective. By using obfuscated code and constantly changing their code, polymorphic malware strains can infect information systems without being detected by solutions such as traditional malware, which is a key asset from the perspective of cyber criminals.</p>

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Polymorphic packer</i></b>	A software tool used for bundling up different types of malware in a single package (for example, in an email attachment). Malicious actors use polymorphic packers because the packers are able to transform over time, so they can remain undetected by traditional security solutions for longer periods of time.
<b><i>Pop-up ad</i></b>	Pop-up ads are windows used in advertising. They appear on top of a browser window when on a website, and they are often annoying and intrusive. While pop-ups are not malicious by nature, sometimes they can become infected with malware if a cyber attacker compromises the advertising networks that are delivering the pop-ups. (Close a pop-up window by simultaneously depressing the ALT and F4 keys while in the window.)
<b><i>Portable electronic devices, portable electronic media</i></b>	Any electronic device or electronic media designed for easy transport. Examples of these items include but are not limited to: smart phones, tablets, laptops, USB flash media, SD cards, diskettes, CDs, DVDs, external hard drives, etc.
<b><i>Portable storage device</i></b>	A storage device that is capable of being physically transported, including but not limited to USB/flash drives/thumb drives, external hard drives, tapes, CDs, DVDs and cameras.
<b><i>Portal</i></b>	The classic intranet portal site functions as an informational hub (i.e., topical tree listing of sites combined with a search engine), aggregating links that connect the portal's constituency of visitors to related information sources. Portals are typically positioned as starting points for users. Private sector examples include AOL and Yahoo.
<b><i>Portfolio management</i></b>	A structured approach to categorize, evaluate, prioritize, purchase, and manage an organization's technology assets in projects based on current and future economic drivers and on the accessible balance of value/risk desired by the organization.
<b><i>Potential impact</i></b>	When a cybersecurity risk is assessed, the loss of the 3 essential factors is considered: confidentiality, integrity and availability. If a risk becomes a cyber attack, it can have low, moderate or high impact.

TERM	DEFINITION
<i>Potentially unwanted application, PUA</i>	There are applications that might be installed on devices which contain adware, which may install toolbars or have confusing purposes. These applications can be non-malicious by nature, but they come with the risk of potentially becoming malicious. Users must seriously consider the risks before they install this type of applications.
<i>Poweliks</i>	Poweliks is a Trojan designed to perform click-fraud operations on the affected PC. Its specific character is given by the fact that it's a type of fileless malware, which makes it very difficult to be detected by traditional, signature-based anti-malware and antivirus solutions. Poweliks installs itself in the Windows registry, where it can inject itself into essential Windows functions. This also helps Poweliks achieve persistence on the infected PC. This malware can be used to also download other threats onto the victim's PC, such as ransomware delivered through malvertising.
<i>Power virus</i>	A type of computer virus is capable of executing a specific code that triggers the maximum CPU power dissipation (heat generated by the central processing units). Consequently, the computer's cooling ability would be impaired and the virus could cause the system to overheat. One of the potential effects is permanent physical damage to the hardware. Power viruses are used both by good actors, to test components, but can also be used by cyber criminals.
<i>Preferred technology standard</i>	A standard which must be complied with by state government, unless the state government entity obtains an exemption from the standard because of technical or other operational deficiencies.
<i>Pretexting</i>	A type of social engineering. It's based on a scripted scenario presented in front of the targets, used to extract PII or some other information. An attacker might impersonate another person or a known figure.
<i>Pretty Good Privacy, PGP</i>	A program for encrypting messages developed by Philip Zimmerman. PGP is one of the most common ways to protect messages on the internet because it is effective, easy to use, and free. PGP is based on the public-key method, which uses two keys - one is a public key that the user disseminates to anyone they would like receive messages from. The other is a private key that the user has to decrypt messages that they receive. To encrypt a message using PGP, a user needs the PGP encryption package, which is available for free from a number of sources. The official repository is at the Massachusetts Institute of Technology.

<b>TERM</b>	<b>DEFINITION</b>
<i>Privacy</i>	The right of individuals to determine for themselves when, how and to what extent information about them is communicated to others.
<i>Private information</i>	As defined in State Technology Law, shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: social security number; driver's license number or non-driver identification card number; or account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account. Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
<i>Private key</i>	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. SOURCE: SP 800-63 through NIST IR7298 Revision 2.
<i>Privileged account</i>	A privileged account is an account which provides increased access and requires additional authorization. Examples include a network, system or security administrator account.
<i>Procedure</i>	Shall mean a set of administrative instructions for implementation of a policy or standard.
<i>Production information system</i>	As per ITEC 7230 §5.10 Production Information System is used to deliver essential services in the normal operating state of the entity.
<i>Profiling</i>	Measuring the characteristics of expected activity so that changes to it can be more easily identified.
<i>Proprietary information</i>	Proprietary information is made of all the data that is unique to an organization and ensures its ability to stay competitive. This can include customer details, technical information, costs, and trade secrets. If cyber criminals compromise or reveal this information, the impact on the organization can be quite severe, as has occurred in major data breaches.

**TERM****DEFINITION*****Protected health information, PHI***

Any information, held or transmitted, concerning a person's health status, medical treatment, or health care payment information (e.g., invoices and statements) created or collected by a covered entity or the business associates of a covered identity. This term applies to health information that can be linked to a specific individual and does not apply to general health statistics applicable to a wide group of people or participants. (Also see 45 CFR 160.103 – Code of Federal Regulations TITLE 45 – Public Welfare Part 160.103 Definitions).

***Proxy server***

A proxy server is a go-between a computer and the internet. Proxies are used to enhance cyber safety because they prevent attackers from invading a computer/a private network directly.

***Public key encryption***

The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. SOURCE: FIPS 201; SP 800-63

***Public key infrastructure, PKI***

A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

***Purge***

The second highest level of sanitizing data that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques. Referenced under NIST 800-88.

**“Q”*****Quad-core, quad-core processor***

A quad-core CPU has four processing cores in a single chip. Similar to a dual-core CPU, but has four separate processors (rather than two), which can process instructions at the same time. Quad-core processors have become popular as the increase in rate of clock speeds for processors have plateaued. By including multiple cores in a single CPU, chip manufacturers can generate higher performance without boosting the clock speed. However, the performance gain can only be realized if the computer's software supports multiprocessing. This allows the software to split the processing load between multiple processors (or cores) instead of only using one processor at a time.

***Quarantine***

The process of storing files containing malware in isolation for future disinfection or examination.

**TERM****DEFINITION**

*Quid pro quo*

A social engineering method that involves people posing as technical support. They make random calls to an organization's employees claiming that they are contacting them regarding an issue. They attempt to have victims take certain actions in exchange for their assistance or service.

**"R"**

***nRedundant-Array-of-Independent Disks, RAID***

A method of storing duplicate data on two or more hard drives. Used for data backup, fault tolerance, to improve throughput, increase storage functions, and to enhance performance by combining two or more hard drives and a RAID controller into a logical unit. The OS sees RAID as a single logical hard drive called a RAID array. The configurations listed below provide the following:

The primary benefit of using RAID is preserving data stored on failed drives. RAID levels use data mirroring, striping and parity, or a combination of those techniques. In most cases, increases in performance or reliability raise the cost of protecting data on the drives. Mirroring occurs when data is written to more than one drive simultaneously, while striping means data is spread across drives in chunks. Parity is a way to make sure data has successfully been written when it is moved from one drive to another.

**RAID 0** - (also known as a stripe set or striped volume) splits data (stripes) evenly across two or more disks, without parity information, redundancy, or fault tolerance. Since RAID 0 provides no fault tolerance or redundancy, the failure of one drive will cause the entire array to fail. Because data is striped across all disks, the failure will result in total data loss. This configuration is typically implemented with speed as the intended goal. RAID 0 is normally used to increase performance, although it can also be used as a way to create a large logical volume out of two or more physical disks.

**RAID 1** - See Disk Mirroring.

**RAID 2** - Rarely used. A central controller synchronizes the disks by making them spin at the same angular orientation so that they all reach the index simultaneously. RAID 2 uses bit-level striping and each sequential bit is placed on a different hard drive. The error correcting code used is the Hamming code parity, which is calculated across bits and stored separately in at least a single drive.

**RAID 3** - Not commonly used. Consists of byte-level striping with a dedicated parity disk. One of the characteristics of RAID 3 is that it generally cannot service multiple requests simultaneously, which happens because any single block of data will, by definition, be spread across all members of the set and will reside in the same physical location on each disk. Therefore, any I/O operation requires activity on every disk and usually requires synchronized spindles.

**RAID 4** - Consists of block-level striping with a dedicated parity disk. As a result of its layout, RAID 4 provides good performance of random reads, while the performance of random writes is low due to the need to write all parity data to a single disk.

**RAID 5** - Most often used when mirroring is not used. Consists of block-level striping with distributed parity. Unlike in RAID 4, it is more robust in that parity information is distributed among the drives. It requires that all drives but one be present to operate. Upon

failure of a single drive, subsequent reads can be calculated from the distributed parity such that no data is lost. RAID 5 requires at least three disks. In comparison to RAID 4, RAID 5's distributed parity evens out the load of a dedicated parity disk among all RAID members. Additionally, write performance is increased since all RAID components participate. Although it will not be as efficient as RAID 0 setup, because parity must still be written, there is no longer a delay in the process.

**RAID 6** – Rarely used. According to the Storage Networking Industry Association it is “any form of RAID that can continue to execute read and write requests to all of a RAID array's virtual disks in the presence of any two concurrent disk failures.”

Additionally, there are the nested levels such as RAID 50, RAID 60 and RAID 10 in which it combines two RAID levels to gain advantages from both. Nested levels are uncommon due to their cost, limited performance, and requirement for additional equipment.

**RAID 10** - Combines the mirroring of RAID 1 (redundancy) with the striping of RAID 0 (high performance).

Level	Minimum drives	Fault tolerance	Pros & Cons
RAID 0	2	None	+ Write/Read speed. - No redundancy.
RAID 1	2	n – 1 drive failures	+ More secure. - Certain cases data loss only as large as smallest drive.
RAID 2	3	One drive failure	+ Data loss can be recalculated. - Expensive - Inefficient - Does not use standard method of mirroring, striping, or parity. - Not often used.
RAID 3	3	One drive failure	+ High throughput for large data + Resistant to disk failure and breakdown. - Disk failures decrease throughput
RAID 4	3	One drive failure	+ Very high performance. Fault tolerance.

**TERM****DEFINITION**

			<ul style="list-style-type: none"> <li>- Lower capacity/High cost.</li> <li>- Limited scalability</li> </ul>
RAID 5	3	One drive failure	<ul style="list-style-type: none"> <li>+ advantages of data storage redundancy along with a high level of performance.</li> <li>+ high degree of fault tolerance</li> </ul>
RAID 6	4	Two drive failures	<ul style="list-style-type: none"> <li>+ Even higher redundancy and read performance.</li> <li>- Lower performance with servers performing large amounts of write operations.</li> </ul>
Nested RAID Configurations combine two configurations such as 1 and 0 to make 10 or 5 and 0 to make 50.			
RAID 10	4	Half, in theory	<ul style="list-style-type: none"> <li>+ High performance, fault tolerance</li> <li>- lower capacity, cost, and limited scalability.</li> </ul>
RAID 50	12-24	Depends	<ul style="list-style-type: none"> <li>+ Improves RAID 5 writes</li> <li>+ Better fault tolerance</li> <li>- Cost</li> <li>- All data is lost if a second drive fails in the same parity group before data from the first failed drive has finished rebuilding.</li> </ul>

***Ransomware***

A type of malware which encrypts all the data on a PC or mobile device, blocking the data owner's access to it. After the infection happens, the victim receives a message advising them a certain amount of money must be paid (usually in Bitcoins) in order to get the decryption key. Usually, there is also a time-limit for the ransom to be paid. There is no guarantee that when a victim pays the ransom, they will get the decryption key. The most reliable solution is to regularly back up the data in at least 3 different places.

***Real-time reaction***

A type of immediate reaction and response to a spotted compromise attempt as it is occurring. The attempted compromise is acted on in real time so the victim can be protected immediately against unauthorized network access.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Reissuance</i></b>	A new credential that is created with a new identity and/or a new token. For example, a password token is re-issued by having the user select a new password.
<b><i>Registration authority, RA</i></b>	A trusted entity that establishes and vouches for the identity of an applicant to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP.
<b><i>Relying party</i></b>	An entity that relies upon the claimant's token and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.
<b><i>Remote access</i></b>	Any access coming into the KRGC network from outside the KRGC's private, trusted network. Any and all wireless networks are considered remote access.
<b><i>Remote Access Trojan, RAT</i></b>	A Trojan that uses the victim's access permissions and infects computers to give cyber attackers unlimited access to the data on the PC. Cyber criminals can use RATs to exfiltrate confidential information. RATs include backdoors into the computer system and can enlist the PC into a botnet, while also spreading to other devices. Current RATs can bypass strong authentication and can access sensitive applications, which are later used to exfiltrate information to cyber criminal controlled servers and websites.
<b><i>Remote diagnostics and maintenance</i></b>	A maintenance service carried on by authorized companies/individuals who use the internet to use a VPN for access to conduct maintenance or perform diagnostics.
<b><i>Renewal</i></b>	The usage or validity period of the token and credential is extended without changing the token or re-verifying the user's identity. Examples of tokens that would be renewed or extended include hard tokens, out of band tokens, one time passwords, and soft tokens.
<b><i>Replay attacks</i></b>	A type of attack that uses authentication data that cyber criminals have previously gathered to re-transmit this confidential information.
<b><i>Residual risk</i></b>	A type of risk that remains after all available security measures and tactics have been applied. Because there is no such thing as 100% secure, a residual risk remains for each identifiable cyber threat.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Resilience</i></b>	An organization's or system's ability to restore its ability to function and achieve its objectives during and after a cyber attack or other transformations. Resilience includes creating contingency plans, constantly evaluating risk management, and planning for every crisis scenario.
<b><i>Restricted-use information, RUI</i></b>	Includes PFI, PII, and PHI as defined in this Cybersecurity Policy, as well as other regulated data (e.g. tax or criminal justice information) or information that agencies designate as restricted-use information due to their confidential or sensitive nature (e.g. physical or logical security information for state agencies and their systems).
<b><i>Revalidate</i></b>	Reconfirming the validation process for a previously validated electronic signature.
<b><i>Reverse engineering</i></b>	A technique heavily used by cybersecurity researchers who constantly take malware apart to analyze it. This way, they can understand and observe how the malware works and can devise security solutions that can protect users against that type of malware and its tactics. This is one of the most valuable activities in cybersecurity intelligence gathering.
<b><i>Risk</i></b>	A function of the likelihood that a given threat will exploit a potential vulnerability and have an adverse impact on an organization.
<b><i>Risk assessment</i></b>	The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.
<b><i>Risk management</i></b>	The process by which an organization manages its cybersecurity risks to decrease their potential impact and take the adequate measures to avoid cyber attacks. Conducting a risk assessment is also part of the process, as well as the risk mitigation strategy and all the procedures that must be applied in order to ensure proper defenses against cyber threats. This is a continuous process and should be viewed as a cycle.
<b><i>Risk mitigation</i></b>	The process by which risks are evaluated, prioritized, and managed through mitigation tactics and measures. Since any entity has a dynamic environment, a periodical revision should be a defining characteristic of the risk mitigation process.

TERM	DEFINITION
<i>Rogue security software</i>	Rogue security software (usually antivirus) is a common internet scam used by cyber criminals to mislead victims and infect their PCs with malware. Malicious actors could also use fake antivirus to trick victims into paying money or extort them (like ransomware does) into paying for having the rogue software removed. So please only buy security software from trusted vendors or from the software makers themselves.
<i>Rogueware</i>	A type of deceitful malware which claims to be a trusted and harmless software program (such as antivirus). Cyber criminals use rogueware to harvest data from their victims or to trick them into paying money. Often, rogueware also includes adware functions, which adds a burden and a potential risk to the infected PC.
<i>Root cause analysis</i>	The process used to identify the root causes for certain security risks in an organization. This must be done with the utmost attention to detail and by maintaining an objective perspective.
<i>Rootkit</i>	A type of malicious software (but not always) which gives the attackers privileged access to a computer and is activated before the operating system boots up. Rootkits are created to conceal the existence of other programs or processes from being spotted by traditional detection methods. For example, rootkit malware is capable of covering up the fact that a PC has been compromised. By gaining administrator rights on the affected PC (through exploits or social engineering), attackers can maintain the infection for a long time and are notoriously difficult to remove.
<i>Router</i>	A network hardware device that routes data (hence the name) from a LAN to another network. This unit essentially bridges between the two networks. Since it is bridging, it analyzes the contents of data packets transmitted within a network or to another network. Routers determine whether the source and destination are on the same network or whether data must be transferred from one network type to another, which requires encapsulating the data packet with routing protocol header information for the new network type.

TERM	DEFINITION
<i>Secure/Multipurpose Internet Mail Extensions, S/MIME</i>	A new version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's (Rivest-Shamir-Adleman) public-key encryption technology. It is expected that S/MIME will be widely implemented, which will make it possible for people to send secure e-mail messages to one another, even if they are using different e-mail clients.
<i>Safeguards</i>	This refers to a set of protection measures that have to meet an information system's core security requirements, in order to ensure confidentiality, integrity, and availability. This includes everything from employee security to ensuring the safety of physical structures and devices, to management limitations and more.
<i>Sanitizing media or data</i>	Refers to a procedure that renders access to target data on the media infeasible for a given level of effort. It is done to ensure confidentiality, after the need of the data or media is no longer desired.
<i>Scareware</i>	A type of malware (or rogueware) that employs social engineering to intimidate and confuse the victims through shock, anxiety, fear and time restrictions. The objective is to maliciously persuade the victims into buying unwanted software. The software could be rogue security software, ransomware or other type of malware. For example, malicious actors often try to manipulate users that their computer is infected with a virus and that the only way to get rid of it is to pay for, download and install a fake antivirus, which, of course, turns out to be the malware itself.
<i>Scavenging</i>	The action of trying to find confidential or sensitive data by searching through a system's data residue.
<i>Screen reader</i>	A software application installed on the client machine which scans all textual data and reads it back aloud to the user through a synthesized voice.
<i>Secure File Transfer Protocol, SSH File Transfer Protocol</i>	A network protocol for accessing, transferring and managing files on systems. SFTP allows the secure transfer of sensitive information. The transfer of files and requires that the client be authenticated by the server. Commands and data are encrypted to prevent passwords and other sensitive information from being exposed to the network in plain text.

<b>TERM</b>	<b>DEFINITION</b>
<i>Secure Sockets Layer, SSL</i>	A protocol developed by Netscape for transmitting private documents via the internet. SSL works by using a private key to encrypt data transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, Webpages that require an SSL connection start with https: instead of http:. SSL has been approved by the Internet Engineering Task Force (IETF) as a standard.
<i>Security controls</i>	A set of safeguards designed to avoid and mitigate the impact of cybersecurity risks that an organization has.
<i>Security impact analysis</i>	An organization should always conduct a security impact analysis to determine if certain changes to the information systems have influenced and impacted its security state.
<i>Security level</i>	The degree of trust that is associated with a user account, based upon Identification Method; one of the attributes of a user account.
<i>Self-registration</i>	The degree of trust that is associated with a user account, based upon Identification Method; one of the attributes of a user account.
<i>Security requirements</i>	Policies derived from multiple sources and make up for the security necessities of an information system, in order to ensure confidentiality, integrity, and availability of the information that is managed, transmitted or stored in the system.
<i>Sensitive information</i>	Information that is not available for everyone to access and is confidential for a certain category of users, who can view, access and use this data. This type of information is protected for reasons related to legal or ethical issues. Examples include: personal identification numbers, health information, education records, trade secrets, credit card information, etc.
<i>Sensitivity</i>	A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.
<i>Server-side image map</i>	A file which is directly read from the server by the browser which contains HTML code that provides coordinates to "hot spots" users may click on inside a given image.
<i>Session cookie</i>	A cookie that is erased during browser operation or when the browser is closed.

TERM	DEFINITION
<i>Shared secret</i>	In the context of this Trust Model a “shared secret” refers to secret information shared by a user for the purpose of confirming that user’s identity. Shared secrets are often used to authenticate a user for the purposes of conveying a credential or resetting a credential such as a password.
<i>Shylock</i>	Shylock is a banking malware created to steal users’ banking credentials for fraudulent purposes. Shylock is based on the leaked Zeus code and acts similar to Zeus GameOver (created based on the same malicious code), because it uses a (DGA) Domain generation algorithm to hide its traffic and remain undetected by traditional antivirus and anti-malware solutions. Shylock is delivered mainly through drive-by downloads on compromised websites which are hit by malvertising, but also through malicious JavaScript injects.
<i>Significant change</i>	Those changes that could impact or affect the security (e.g. Changing devices such as firewalls, routers, switches and servers).
<i>Signature</i>	A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.
<i>Simulation, simulator</i>	A functional exercise staff member who simulates or represents non-participating individuals or organizations whose input or participation is necessary to the flow of the exercise.
<i>Skimming</i>	Occurs when a malicious actor uses a tag reader in an unauthorized manner, in order to collect information about a person’s tag. The victim never knows or accepts to be skimmed. An example is credit card skimming which consists of the illegal collection of data from a card’s magnetic stripe. This information can then be copied onto a blank card’s magnetic stripe and used by malicious actors to make purchases and withdraw cash in the name of the victim.
<i>Smart card</i>	A hardware token that incorporates one or more integrated circuit chips to implement cryptographic functions and possesses some inherent resistance to tampering.
<i>Sniffer</i>	A tool used to monitor packet traffic over a network, usually used legitimately, to detect issues with the data flow. But it can also be used by malicious individuals, to harvest data that is transmitted over a network.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Social engineering</i></b>	The act of exploiting human weaknesses to gain control or obtain information. Social engineering relies on manipulating individuals rather than hacking computer systems to penetrate a target's system. A form of psychological manipulation used to persuade people to perform certain actions or give away sensitive information. Manipulation tactics include lies, psychological tricks, bribes, extortion, impersonation, and other type of threats. Often used to extract data and gain unauthorized access to information systems, for a single, private users or which belong to organizations.
<b><i>Source record</i></b>	ITEC 7230 §5.14 defines as the authoritative instance of a record within an entity.
<b><i>Sound mixer</i></b>	A device which takes two or more audio signals, mixes them together and provides one or more output signals.
<b><i>Spam</i></b>	Unsolicited emails or other types of messages sent over the internet. Spam is often used to spread malware and phishing, which is why users should never open, reply to, or download attachments from spam messages. Spam can be sent in the form of emails, instant messages, comments, etc.
<b><i>Spam filter</i></b>	A type of program which can analyze emails and other types of messages (i.e. instant messages) to weed out spam. If spam filtering software decides to categorize a message as spam, it will move that message to a dedicated folder.
<b><i>Spear phishing</i></b>	A cyber attack that aims to extract sensitive data from a victim using a very specific and personalized message. This message is usually sent to individuals or companies, and it's extremely effective, because it's very well planned. Attackers invest time and resources into gathering information about the victim (interests, activities, personal history, etc.) in order to create the spear phishing message (which is usually an email). Spear phishing uses the sense of urgency and familiarity (appears to come from someone the user knows) to manipulate the victim, so the target does not think they have time to double check the information, or would look foolish to do so.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Spillage</i></b>	System changes that includes, but is not limited to: adding, deleting, modifying features or functionality to existing systems; substantial redesign of the existing system or environment; or other modifications that could substantially affect the system security. Typically, data is moved from a safe, protected system to another system which is less secure.
<b><i>Spoofing email</i></b>	A compromise attempt during which an unauthorized individual tries to gain access to an information system by impersonating an authorized user. For example, email spoofing occurs when cyber attackers send phishing emails using a forged sender address. A user might believe that they are receiving an email from a trusted entity, which causes them to click on the links in the email, but the link may end up infecting the PC with malware.
<b><i>Spy-phishing</i></b>	A type of malware that employs tactics found in both phishing and spyware. By combining these cyber threats, spy-phishing is capable of downloading applications that can run silently on the victim's system. When the victims open a specific URL, the malware will collect the data the victim puts into that website and send it to a malicious location (like a web server). This technique is used to extend the duration of the phishing attack, even after the phishing website has been taken down.
<b><i>Spyware</i></b>	A type of malware designed to collect and steal the victim's sensitive information, without the victim's knowledge. Trojans, adware, and system monitors are different from spyware. Spyware monitors and stores the victim's internet activity (keystrokes, browser history, etc.) and can also harvest usernames, passwords, and financial information. Spyware can also send this confidential data to servers operated by cyber criminals, so they can use it in subsequent cyber attacks.
<b><i>Structured Query Language injection, SQL injection</i></b>	A tactic that used code injection to attack applications which are data-driven. The maliciously injected SQL code can perform several actions, including dumping all the data in a database in a location controlled by the attacker. Through this attack, malicious hackers can spoof identities, modify or tamper with data, disclose confidential data, delete or destroy the data, or make it unavailable.

<b>TERM</b>	<b>DEFINITION</b>
<i>Secure Sockets Layer, SSL</i>	An encryption method to ensure the safety of the data sent and received from a user to a specific website. Encrypting this data transfer ensures that no one can snoop on the transmission and gain access to confidential information, such as credit card information. Legitimate websites use SSL (URL beginning with https) and users should avoid inputting their data in websites that do not use SSL.
<i>Standard</i>	Sets of rules for implementing policy. Standards specify technologies, methodologies, implementation procedures, and other detail factors.
<i>State</i>	State of Kansas.
<i>State agency</i>	Any department, board, bureau, commission, division, office, council, committee, or office of the state. Excludes the legislature or the judiciary.
<i>State entity</i>	See state government.
<i>State government</i>	Includes all state agencies, departments, offices, divisions, boards, bureaus, commissions and other entities over which the Governor has executive power, as well as the legislative and judicial branches of government.
<i>Stealware</i>	A type of malware which is capable of transferring data or money to a malicious third party. This type of malware typically targets affiliate transactions then uses an HTTP cookie to redirect the commission earned by an affiliate marketer to an unauthorized third party.
<i>Strong authentication</i>	A specific requirement that calls for employing multiple authentication factors from different categories and sophisticated technology to verify an entity's identity. Dynamic passwords, digital certificates, protocols, and other authentication elements are part of strong authentication standards. Strong authentication is regularly used in banking and financial services, where access to an account has to be tied to a real person or an organization.
<i>Succession planning</i>	A strategic approach towards workforce development, ensuring resource continuity by taking proactive steps to train employees and fill resource gaps in anticipated workforce turnover.
<i>Supervisor</i>	An individual who is responsible for day-to-day management or supervision of a user.

<b>TERM</b>	<b>DEFINITION</b>
<i>Supply chain attack</i>	A type of attack aimed to inflict damage upon an organization by leveraging vulnerabilities in its supply network. Cyber criminals often manipulate hardware or software during the manufacturing stage to implant rootkits or tie in hardware-based spying elements. Attackers can later use these implants to attack the organization they are targeting.
<i>Suppression measure</i>	Any action or device used to reduce the security risks in an information system. Part of the risk mitigation process, aimed at minimizing the security risks of an organization or information system.
<i>Suspicious files and behavior</i>	A description of when files exhibit an unusual behavior pattern. For example, if files start copying themselves to a system folder, this indicates that those files may have been compromised by malware. Traditional antivirus solutions incorporate this type of detection to spot and block malware.
<i>Switch</i>	A network device that is used to connect segments of a LAN or LANs and to filter and forward packets among them. Hubs and switches are different in many ways. For one, a switch will have more ports. A hub is passive in that it is just connecting the units, and does not have software to operate. The switch is an active intelligent device and requires software to function. The hub is slower than a switch, and not as sophisticated. Also known as a network switch.
<i>Synchronized text captioning</i>	A text transcript that is synchronized or coordinated in time with the audio and video track.
<i>System</i>	An interconnected set of information resources under the same direct management control that shares common functionality. A system at a minimum includes hardware, software, applications, and communications.
<i>System administrator, sysadmin</i>	A person in charge of all the technical aspects of an information system. This includes but is not limited to configuration, maintenance, ensuring reliability, and obtaining necessary resources for optimal performance of the system while respecting a budget.
<i>System integrity</i>	An information system that is able to perform its dedicated functions at optimal parameters, without intrusion or manipulation (intentional or unintentional).

**TERM****DEFINITION**

***Systems Security Certified Practitioner, SSCP***

A person with entry-level information security certification. The SSCP certification focuses on seven Common Body of Knowledge:

1. Access Controls
2. Security Operations and Administration
3. Risk Identification, Monitoring, and Analysis
4. Incident Response, and Recovery
5. Cryptography
6. Networks and Communications Security
7. Systems and Applications Security

***System service account***

A special user account that an application or service uses to interact with an information system.

**“T”**

***Tailgating***

A method of social engineering in which an unauthorized person sneaks through a door after an authorized person opens the door.

***Tampering***

The intentional activity of modifying the way an information system works in order to force it to execute unauthorized actions.

***Target implementation environment***

The deployment environment in which the new or modified system is installed or fielded for use by a defined set of users after system acceptance is complete. Often referred to as the production environment.

***Targeted threat***

A class of malware destined for one specific organization or industry. Cyber criminals prepare these threats for a long time so that they can extract sensitive information from the target. The threats are carefully documented so that the chance of a successful compromise is as high as possible. Targeted threats are delivered via email (phishing, vishing, etc.), zero-day attacks, and by exploiting other vulnerabilities to penetrate an information system. Governments and financial organizations are the most frequent targets for this type of cyber threat.

***Technology***

A digital, electronic, or similar technical method of achieving a practical purpose or improvements in productivity, including but not limited to, information management, equipment, software, operating systems, interface systems, interconnected systems, telecommunications, data management, networks, and network management, consulting, supplies, facilities, maintenance, and training.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>TeslaCrypt</i></b>	A ransomware Trojan that was first designed to target computers that have specific computer games installed. This strain of cryptoware has since broadened its reach to affect all users (primarily Windows users), not just gamers. As with other ransomware, TeslaCrypt creators use spam to distribute the infection and, once inside the victim's PC, all data on the device will be encrypted and held hostage. The demanded ransom has varied between \$150.00 and \$1,000.00 worth of bitcoins in exchange for the decryption key. In March 2016, TeslaCrypt 4.0 emerged, which featured unbreakable encryption, thus rendering available TeslaCrypt decoders useless.
<b><i>Threat</i></b>	A potential circumstance, entity, or event capable of exploiting a vulnerability and causing harm. Threats can come from natural causes, human actions, or environmental conditions. A threat cannot present a risk if there is no vulnerability to exploit.
<b><i>Threat analysis</i></b>	The process of examining sources of cyber threats and evaluating them in relation to the information system's vulnerabilities. The objective of the analysis is to identify the threats that endanger a particular information system in a specific environment.
<b><i>Threat assessment</i></b>	An evaluation of cyber threats against an organization by categorizing them into types so the threats can be managed, prioritized, and mitigated more easily.
<b><i>Threat event</i></b>	A potentially harmful situation for an information system that can have unwanted consequences.
<b><i>Threat monitoring</i></b>	A continuous process in which security audits and other similar information are gathered, analyzed, and reviewed to determine if certain events in the information system could endanger the system's security.
<b><i>Threat scenario</i></b>	An illustration in which one or more threat actors can mount one or more threat actions in an attempt to compromise a system. A scenario draws information from all available resources and focuses on three key elements: vulnerabilities, threats, and impact. This process helps associate a specific cyber threat to one or more threat sources and establishes priorities.

TERM	DEFINITION
<i>Threat shifting</i>	The process of adapting protection measures in response to cyber attackers' ever-changing tactics. Countermeasures must be constantly updated to meet the challenges posed by polymorphic malware.
<i>Threat source</i>	The objective and method used by cyber attackers to exploit a security vulnerability in order to compromise an information system. Triggering a system vulnerability may happen accidentally or intentionally.
<i>Time bomb</i>	A type of malware that remains dormant on the system for an amount of time until a specific event triggers it. This malware characteristic makes detection by security software more difficult and backups less functional.
<i>Time-dependent password</i>	A password that can be either valid for a limited amount of time or for use during a specific interval in a day. Time-dependent passwords are most often generated by an application and are part of a two-factor or multi-factor authentication mechanism.
<i>Token</i>	Something that a user possesses and controls (typically a key or password) used to authenticate the user's identity. A token incorporates one or more of the three factors of authentication: something a user knows (e.g., user-ID, password, personal identification number (PIN), or passcode); something a user has (e.g., a one-time password authentication token, 'smart card'); or something the user is (e.g., fingerprint, retina scan).
<i>Tracking cookie</i>	This type of cookie is placed on users' computers during web browsing sessions. Their purpose is to collect data about the user's browsing preferences on a specific website, so they can then deliver targeted advertising or to improve the user's experience on that website by delivering customized information.
<i>Traffic analysis</i>	The process by which traffic on a network is intercepted, examined, and reviewed in order to determine traffic patterns, volumes, and extract relevant statistics about it. This data is necessary to improve a network's performance, security, and general management.
<i>Transaction</i>	A discrete event between user and systems that supports a business or programmatic purpose. Typical transaction types are read, write, execute, and purge.

TERM	DEFINITION
<i>Trojan, Trojan horse</i>	A type of malware that acts according to the Greek legend, it camouflages itself as a legitimate file or program to trick unsuspecting users into installing it on their PCs. By doing this, users will unknowingly give unauthorized, remote access to the cyber attackers who created and run the Trojan. Trojans can be used to spy on a user's activity (web browsing, computer activity, etc.), to collect and harvest sensitive data, to delete files, to download other malware onto the PC, and more.
<i>Trust</i>	The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued and the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
<i>Trusted organization</i>	A federal, state, or local government entity with which the state or KRGC has established a business relationship to issue credentials through a service level agreement, memorandum of understanding, or other comparable mechanism, or, a private entity that has a similar contractual relationship with the government entity. The process for issuing credentials must be clearly documented and agreed by the Trust Model's management authority.
<i>Trusted party</i>	An entity with which the state or KRGC has established a business relationship through a service level agreement, memorandum of understanding, contract, or other comparable mechanism.
<i>Trustworthy system</i>	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; that provide a reasonable level of availability, reliability, and correct operation; that are reasonably suited to performing their intended functions; and that enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
<i>Typhoid adware</i>	A cybersecurity threat that employs a man-in-the-middle attack in order to inject advertising into certain webpages that a user visits while using a public network, like a public, non-encrypted Wi-Fi hotspot. The computer being attacked does not need to have adware on it meaning that installing a traditional antivirus will not counteract the threat. While the ads themselves can be non-malicious, they can expose users to other threats like promoting a fake antivirus program that is actually malware or a phishing attack.

TERM	DEFINITION
<i>Unauthorized access</i>	Occurs when someone illegally or illegitimately accesses protected or sensitive information without permission.
<i>Unauthorized disclosure</i>	Occurs when sensitive, private information is communicated or exposed to parties who are not authorized to access the data.
<i>Undue financial or administrative burden</i>	A significant difficulty or expense. In determining whether an action would result in an undue burden, state government entities must consider all resources available for the funding and operation of the service, program, or activity.
<i>URL injection, link injection</i>	Occurs when a cyber-criminal creates new pages on a website owned by someone else that contain spam words or links. These pages sometimes contain malicious code that redirects users to other webpages or makes the website's web server contribute to a DDoS attack. URL injection typically occurs because of vulnerabilities in server directories or software used to operate the website, such as an outdated WordPress or plugins.
<i>USA PATRIOT Act</i>	A federal statute passed in October 2001 that extended existing anti-money-laundering legislation beyond drug trafficking to terrorism funding. USA PATRIOT Act is an acronym for Unifying and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.
<i>User</i>	Any KRGC employee or other individual who is authorized to access a KRGC system for a legitimate government purpose.
<i>User ID</i>	A unique alphanumeric identifier, a username, by which a person is identified to a computer system or network.

**“V”**

<i>Vaccine</i>	A digital solution which focuses on neutralizing attacks once they gain unauthorized access to an information system. Cyber vaccines exploit flaws similar to how malware works and spreads, so the malware’s distribution and effects can be blocked. A cyber vaccine can train an information system to detect and stop cyber attacks after they have penetrated the system but before the attacker can cause actual damage. Cyber vaccines are a new concept so more must be done to advance them. They have the potential to stop ransomware, block data exfiltration, intercept phishing attacks, block zero-day exploits, and more.
----------------	---

<b>TERM</b>	<b>DEFINITION</b>
<i>Variance</i>	A deviation from a control mandated in these policies.
<i>Vawtrak Neverquest</i>	A classic infostealer malware that aims to mainly steal login credentials for banking portals, either stored on the local device or transmitted from the affected PC, but the malware can also harvest other information from financial institutions. The malware uses the stolen credentials to gain unauthorized access to bank accounts and commit financial fraud. The infostealer malware can also take screenshots of the infected device, capture videos, and launch man-in-the-middle attacks. Vawtrak is delivered through drive-by downloads in compromised websites, by injecting malicious code on legitimate websites, or via phishing campaigns on social media networks and spam.
<i>Verifier</i>	An entity that verifies the claimant's identity by verifying the claimant's possession and control of a token using an authentication protocol.
<i>Video Description</i>	A tool for videos and other visual media to be made accessible to people who are blind or visually impaired by providing descriptive narration of key visual elements in programs.
<i>Virtual Private Network, VPN</i>	A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable users to create networks using the internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
<i>Virus</i>	A type of malicious software code capable of self-replication. A virus needs human intervention to initially run and it can copy itself into other computer programs, data files, or in certain sections of the computer, such as the boot sector of the hard drive. Once this happens, these elements will become infected. Viruses are designed to harm computers and information systems and can spread through the internet through malicious downloads, infected email attachments, malicious programs, files or documents. Viruses can steal data, destroy information, log keystrokes, and more.

**TERM****DEFINITION**

<b><i>Virus hoax</i></b>	A message that warns about a non-existent computer virus threat. This is usually transmitted via email and tells the recipients to forward it to everyone they know. Computer hoaxes typically do not directly cause damage, but their intent is not innocent, as they exploit users' lack of knowledge, concern, or ability to investigate before users take the action described in the hoax.
<b><i>Vishing, Voice over IP phishing, VoIP phishing</i></b>	A form of phishing performed over the telephone or VoIP technology such as Skype. Unsuspecting victims are duped into revealing sensitive or personal information on telephone calls, VoIP calls, or voice mail messages.
<b><i>Vulnerability</i></b>	A weakness or hole in a computer security system that the developer or agency did not intend to create, which may allow a cyber attacker to gain unauthorized access to the system and cause damage. Vulnerabilities can be accidentally triggered or intentionally exploited. The difference between a vulnerability and a threat is that a vulnerability is internal and a threat is external. These vulnerabilities, if left unfixed, provide an opportunity for an outside threat to exploit the system, alter performance, or steal data. Vulnerabilities should be solved as soon as they are discovered to prevent cyber criminals from exploiting them.
<b><i>Visual Inspection</i></b>	Inspection of valid current photo ID that contains the applicant's picture and either address of record or nationality (e.g., driver's license or Passport). Inspection will include comparing picture to applicant and recording ID number, address and date of birth.

**“W”**

<b><i>Wi-Fi Protected Access, WPA</i></b>	A security protocol used in Wi-Fi networks. An improvement from WEP because it offers greater protection through more sophisticated data encryption.
<b><i>Wi-Fi Equivalent Privacy, WEP</i></b>	A security protocol used in Wi-Fi networks. WEP is designed to provide a wireless LAN with a level of security similar to that of a wired LAN. WEP-secured networks are typically protected by passwords.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Wabbits</i></b>	One of four main classes of malware, the other three being viruses, worms, and Trojans. Wabbits are a form of computer program that replicates itself on the local system. Wabbits can be programmed to have malicious effects. One type of wabbit is a fork bomb that is a DoS attack against a computer that uses the fork function. A fork bomb quickly creates a large number of processes which eventually crashes the system. Wabbits do not attempt to spread to other computers across network.
<b><i>Watering Hole</i></b>	A computer attack strategy that was first detected in 2009 and 2010. Victims are particular, targeted groups, such as a company, organization, agency, industry, etc. The attacker spends time to gain strategic information about the target by observing which legitimate websites are visited more often by members of the group. The attacker then exploits a vulnerability and infects one of those trusted websites with malware, without the knowledge of the site's owner. Eventually, someone from the targeted organization will visit the infected website and their computer will become infected. By doing this, the attacker gains access to the target's entire network. These attacks are successful because of persistent vulnerabilities in website technologies that, even with popular systems like WordPress, make it relatively easy to stealthily compromise websites.
<b><i>Web bug, web beacon, pixel tag</i></b>	A small, transparent GIF image, usually not bigger than 1 pixel. A web bug is embedded in an email or webpage and is typically used in connection with cookies. Web bugs are designed to monitor a user's activity and they load when a user opens an email or visits a website. Most common uses are marketing-related, for email tracking (to monitor if and when recipients open emails), web analytics (to monitor how many people visited a website), advertisement statistics (to determine how often an ad appears or is viewed), IP address gathering, or determining browser type used.
<b><i>Web content filtering software</i></b>	A program that screens incoming webpages and restricts or controls its content. The software can be used by governments to censor the internet from its citizens, by ISPs to block copyright infringement, by employers to block personal email clients or social media networks, by a school or by parents to block inappropriate content for children, etc. This software can block pages that include copyright infringement material, pornographic content, or social networks, etc.

<b>TERM</b>	<b>DEFINITION</b>
<b><i>Webattacker</i></b>	A do-it-yourself malware creation kit that demands minimal technical knowledge to manipulate and use. It includes scripts that simplify the task of infecting computers and spam-sending techniques.
<b><i>Whaling</i></b>	A form of sophisticated phishing that has the objective of collecting sensitive data about a target. Whaling differs from phishing because whaling exclusively targets high-profile, famous, and wealthy targets, including celebrities, CEOs, top-level management, and other powerful or rich individuals. By using the phished information, fraudsters and cyber criminals can trick victims into revealing more sensitive data, extort victims, or commit financial fraud.
<b><i>Whitehat hacker, ethical hacker</i></b>	Hackers who are typically cybersecurity specialists, researchers, or skilled techies who find security vulnerabilities for organizations and notify those organizations so that they can fix the issue. Unlike Blackhat hackers, they do not exploit vulnerabilities except for demonstration purposes. Companies often hire Whitehat hackers to test their security systems, which is known as penetration testing.
<b><i>Whitelist</i></b>	A list of email addresses or IP addresses that are considered to be spam-free. A whitelist is the opposite of a blacklist, which contains a list of blocked users. Spam filters use both whitelists and blacklists of senders to help detect spam emails.
<b><i>Wireless communications infrastructure</i></b>	Infrastructure that includes the land, wireless communications towers, buildings, rooftops, antenna support structures, equipment shelters, and other site infrastructures which could be used to support transmission or receiving equipment for wireless communications where such infrastructure is: (1) is owned, leased or otherwise controlled by a state government entity or where the grant of a lease, license or permit for use of such infrastructure requires the approval of such entity; and (2) represents expenditures or revenue, in the aggregate, equal to or greater than seventy-five thousand dollars (\$75,000) over the entire contract terms.
<b><i>Wireless technology</i></b>	Technology that permits the transfer of information between separated points without physical connection. Currently wireless technologies use infrared, acoustic, radio, and optical frequencies.
<b><i>Workforce</i></b>	State employees and other persons whose conduct, in the performance of work for the state, is under the direct control of the state entity, whether or not they are paid by the state entity.

**TERM****DEFINITION*****Worm***

One of the most common types of malware. Similar to a virus, but spreads differently. Worms have the ability to spread independently and self-replicate automatically by exploiting operating system vulnerabilities, while viruses rely on human activity in order to spread. A worm is usually caught via mass emails that contain infected attachments. Worms may also include payloads that damage host computers, commonly designed to steal data, delete files, send documents via email or install backdoors.

**“X, Y”*****Yubico Key***

A two-factor-authentication key used by KRGC.

**“Z”*****Zero-day attack,  
zero-hour attack***

Attacks that exploit vulnerabilities in computer software that cyber criminals have discovered and software makers have not patched. These are often exploited by cyber attackers before the software or security companies become aware of the vulnerabilities. Zero-day attacks are sometimes discovered by security vendors or researchers and kept private until the organization patches the vulnerability.

***Zero-day  
virus/malware***

A computer virus, Trojan horse, or other malware that was previously unknown by software developers or by traditional antivirus producers. This means the vulnerability is undisclosed to the public, though it might be known and quietly exploited by cyber attackers. Because a zero-day not known yet, this means patches and antivirus software signatures are not yet available for it and there is little protection against an attack.

***Zeus, Zbot***

A notorious banking Trojan which infects Windows users in order to retrieve confidential information from the infected computers. Once installed, it tries to download configuration files and updates from the internet. Its purpose is to steal private data from the victims, such as system information, passwords, banking credentials, or other financial details. Zeus can be customized in a variety of methods to gather banking details in specific countries. By obtaining this information, cyber criminals can log into banking accounts and make unauthorized money transfers through a complex network of computers, thereby committing banking fraud. Operation Tovar, carried out in 2014, took down the Zeus network of control and command servers, because it had caused millions of dollars in damages and spread very quickly.

**TERM****DEFINITION**

***Zeus GameOver,  
Zeus P2P***

A variant of the ZeuS/Zbot family which relies on a peer-to-peer botnet infrastructure to work. Zeus GameOver was used by cyber criminals to collect financial and other personal information in order to access the victims' online bank accounts. GameOver Zeus is estimated to have infected one million users around the world and it was taken down in 2014 by Operation Tovar.

***Zip bomb, zip of  
death,  
decompression  
bomb***

A malicious archive file. When uncompressed, it expands dangerously, requiring large amounts of time, disk space, and memory which causes the system to crash. A zip bomb is typically a small file, less than a few hundred kilobytes, in the form of a loop, which will continuously unpack itself until all system resources are exhausted. It is designed to disable antivirus software so that a more traditional virus can be sent after to infect the system without being detected.

***Zombie computer***

A computer connected to the internet, which in appearance is performing normally, but can be controlled by a hacker who has remote access to it and sends commands through an open port. Zombies are mostly used to perform malicious tasks, such as spreading spam or other infected data to other computers or launching DoS attacks, without the owner's awareness.

***Zombie attack***

A form of DoS attacks. A zombie attack originates from an insecure web server on which malicious code was placed. The attack is triggered simultaneously with other zombie servers to launch an overwhelming number of requests toward a targeted web site, which becomes overwhelmed and cannot provide legitimate requests.

<b>Subject</b>		<b>Number Draft #3</b>
<b>CYBERSECURITY POLICY          RISK MANAGEMENT, DATA MANAGEMENT &amp;          DATA CLASSIFICATION</b>		<b>2020-06</b>
<b>Adopted</b> September 11, 2020	<b>Last Revision</b> April 30, 2020	<b>Rescinds</b> N/A
<b>Commission Authorization</b>		
<b>Chairman Brandon Jones</b>	<b>Date</b>	

**I. Purpose/Background**

- A. The purpose of this policy and procedure is to meet the requirements of the Kansas Cybersecurity Act of 2018 and subsequent ITEC 7230 mandates. It assists in ensuring that KRGC’s protected information is not erroneously released and that the three elements of the CIA triad (Confidentiality, Integrity and Accessibility) are met.
- B. The process of classifying information pursuant to this policy serves as a basis for staff to evaluate the retention and disposition schedules currently in effect for its records and, where appropriate, consider revising those schedules as a means of managing the records that must be protected by the agency. Similarly, the classification process facilitates the accurate and efficient application of the exemptions from disclosure enumerated in the Kansas open records act by providing a framework for a comprehensive assessment of the agency’s information assets.

**II. Introduction**

- A. This standard outlines a classification process and provides procedures for classifying information in order to uniformly protect information entrusted to KRGC. However, if there is any doubt on the classification of data, the classification will default to the highest level of restriction.
- B. The scope of this standard includes information through its entire life cycle (i.e., generation, use, storage and disposition). It covers information in any form including electronic, paper, voice, video or other physical forms.

### III. Policy

- A. KRGC has appointed responsibility, method, and task to ensure proper governance of data. This will be carried out through the use of a Trustee and Custodian assigned to restricted data assets.
- B. A Data Trustee will be assigned to data assets. For KRGC, data assets will be identified as any intellectual property, or any number of files which contain, or may be projected to contain, Source Records with Restricted-Use Information.
  1. The Data Trustees are the owners of the data, and they are tasked to perform the following:
    - a. Determine the potential impact to the affected entity, individuals, and the State in the event of a loss of confidentiality, integrity, and availability of the Information Asset.
    - b. Classify the asset in accordance with the entity's Information Asset classification standard.
    - c. Ensure that the asset is handled in accordance with the entity's Information Asset handling standard.
    - d. Ensure that adverse events are reported to the KRGC Information Security Officer (ISO).
    - e. The Trustee shall also appoint Information Asset custodians. The custodian shall perform the following tasks:
      - i. approve all access and use of the Information Asset;
      - ii. recertify annually the classification, access, users, and custodians of the Information Asset;
      - iii. implement and operate the safeguards and controls for Information Assets as directed by Information Asset trustees.
    - f. The Data Trustee shall also become a part of the Board of Trustees. Their responsibilities as a combined unit is defined and identified in policy 2020-21.
  2. The IT and cybersecurity unit shall conduct an audit of the KRGC IT system and determine the vulnerabilities (Risks) in the system. All the risks identified shall be documented in a log, from here on referred to as the Risk Register.
    - a. Within 30 days of identification of any risk, KRGC Management Team shall accept a plan to a process that addresses risk identification, tracking, mitigation, reporting, and acceptance.

- i. This will be an issue in executive staff meeting until addressed.
      - ii. When addressed, the executive staff will direct the IT Department and cybersecurity unit to enter the method in the change log and Risk Register.
    - b. The Risk Register will be used to document and track all outstanding risks.
    - c. Quarterly, KRGC will review existing risks and repeat the process of items a through b.
  3. Change logs and Event logs shall be maintained. They will be in one database, but used for different occurrences. The logs will also include any exceptions noted that were in violation of the cybersecurity policies. KRGC will log all variances to this policy in the event log, as well as Exceptions to the requirements in this policy.
- C. Data Hierarchy - KRGC has developed a hierarchical Information Asset classification based on the needs of the agency to perform its tasks and the needs of the user. All data must be classified according to the KRGC data classification schema below and protected according to KRGC data security standards. This policy applies to data in all formats or media.

Data and information assets are classified according to the information they contain and the risks associated with data being stored or processed. Data with the highest risk needs the greatest level of protection to prevent compromise; data with lower risk requires proportionately less protection. Three levels of data classification will be used to classify KRGC Data based on how the data is, or could be, used. This takes into account the sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

Data assets are typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements (e.g. an employee file system will contain an employee's financial information as well as their social security number.) Consequently, the classification of the most sensitive element in a data collection will determine the data classification of the entire collection. Below are the acceptable levels of classifications.

1. **Public** - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the agency, affiliates, or individuals. Public data generally have a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include, but are not limited to:
  - a. Published casino financial reports

- b. Commission minutes
  - c. Consent agenda
  - d. KRGC's public web site.
  - e. Gaming machines approved for Kansas
  - f. Press releases.
2. **Agency Only (AO) - Confidential or Agency Only** - Data intended for use within the internal agency only, with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data are generally not made available to parties outside the KRGC community. Unauthorized disclosure could adversely impact the Agency, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. Examples include:
- a. Financial accounting data that does contain confidential information.
  - b. Casino operating information
  - c. Casino security information
  - d. KRGC Information Technology Information System information
  - e. Information technology transaction logs.
  - f. Employee ID number (with limitations)
  - g. Table of internal usage

User Category	Privileges & Responsibilities
Department Users (Employees)	Access to application and databases as required for job function.
System Administrators	Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only.
Security Administrator	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
Systems Analyst/Programmer	Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices.
Contractors/Consultants	Access to applications and databases as required

	for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to agency information and systems must be approved in writing by the agency Executive director and requires Trustee approval
Other Agencies and Business Partners	Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws. <b>Also requires Trustee approval</b>
General Public	NEVER

3. FLEO (For Law Enforcement Only) – This is Law Enforcement intelligence information on criminal activity, such as known individuals in the area who are involved in criminal activity. It also includes information developed by the Electronic Gaming Unit on how to cheat a slot machine. It does not include any information containing information that would place it in the confidential or higher level such as controlled, or restricted.
4. CUI (Controlled Unclassified Information) – Designation of information that, though unclassified, often requires strict controls over its viewing, and distribution. CUI is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of CBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not.
5. Restricted Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Steward is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the Agency or affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations or Agency contracts. Confidential data have a very high level of sensitivity. Examples include:
  - a. Any Social Security Number, or any identifier which uses a social security number
  - b. Credit card number
  - c. Personal identity information (PII). K.S.A. § 21-6107: Crimes involving violations of personal rights defines PII as including, but not limited to: an individual's name; date of birth; address; telephone number; driver's license number or card or nondriver's identification number or card; social security

number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information. For KRGC's purposes, PII also includes data with a name in combination with a passport number

- d. Passport number
  - e. Personnel records
  - f. Medical records
  - g. Authentication tokens (e.g., personal digital certificates, passwords, biometric data)
6. Confidential- is not a category per se. It is a generalized statement. It means any information not to be released outside the agency. It is an umbrella term for the classifications. It could also include information that the release of could display a lack of professionalism or integrity (e.g., another agency provides information about a gambling situation and advises they do not want it released any further without their permission.)
7. Handling caveats - Since KRGC is a law enforcement agency, there is a possibility information would have additional restrictive caveats. These are constantly changing, but can include (in abbreviated form) a requirement that the document not be shared with a civilian contractor, only shared with law enforcement, or not leave a specific room. These restrictions are not classifications in and of themselves; rather, they restrict the dissemination of information within those who have the appropriate clearance level and possibly the need to know the information.

For ease of use, caveats and abbreviations have been adopted that can be included in the summary classification marking (header/footer) to enable the restrictions to be identified at a glance. They are sometimes known as Dissemination Control Abbreviations (e.g., FOUO: For Official Use Only. Used for documents or products which contain material which is exempt from release under the Freedom of Information Act, but contain information that should not be released to the public on operations (e.g. violations).

Classification level and caveats are typically separated by "/" in the summary classification marking. For example, the final summary marking of a document might be "Classified//Law Enforcement Only".

8. Proprietary Data - Classification of data provided to or created and maintained by KRGC on behalf of a third-party, such as a corporation or government agency, will

vary depending on contractual agreements and/or relevant laws, regulations, or agreements.

The classification and security standards for proprietary data owned by the third-party will be defined by the third-party. Should KRGC have proprietary data, it would be classified and protected according to these standards

Proprietary Data would also include the use of intellectual work, such as writings, drawings, recordings, through reproduction, distribution, or display of without permissions, infringing on certain exclusive rights granted to the copyright holder. See KRGC Policy 2020-04 for details.

9. Default level - If a KRGC staff member is receiving the data, they shall address it with the highest security level until it is classified by a trustee responsible for the data. All data is considered Restricted until it is classified.
10. Classification - Using the cybersecurity CIA Triad (Confidentiality, Integrity, and Accessibility) goals, KRGC will be assisted in the classification of the data assets sensitivity. Each databank will be evaluated based on the three groups of questions in the checklist provided in Appendix "A". Explanation of the categories will be found in Appendix "B".
11. Determination of Controls - Once the information is classified, a listing of baseline controls for each type of classification can be found in the control charts in Appendix A of the Information Security Controls Standard. However, although a data asset does not have a higher classification, it could have as negative of an effect as a higher classification should it be improperly handled or breached.

The trustee may use the considerations in Appendix "C" when determining or considering impact level. They may also consider the following:

- a. Limited impact would:
  - i. cause a degradation in mission capability to an extent and duration that the agency is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
  - ii. result in minor damage to KRGC or third-party assets;
  - iii. result in minor financial loss; or
  - iv. result in minor harm to individuals.
- b. Serious impact would:

- i. cause a significant degradation in mission capability to an extent and duration that the agency is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  - ii. result in significant damage to KRGC or third party assets;
  - iii. result in significant financial loss; or
  - iv. result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
- c. Severe or catastrophic impact would:
- i. cause a degradation in or loss of mission capability to an extent and duration that KRGC is not able to perform one or more of its primary functions;
  - ii. result in major damage to KRGC or third party assets;
  - iii. result in major financial loss to anyone; or
  - iv. result in catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
- d. The information classification process shall include the following:
- i. Identifying information assets
  - ii. Classifying information assets by confidentiality, integrity, and availability (CIA)
  - iii. Determining controls based upon the classification
- e. The trustee shall answer the questions in the Information Asset Classification Worksheet (Appendix A) to determine the classification of their information assets. These check sheets are guides, and common sense should prevail. It is appropriate to recruit and work with subject matter experts who have specific knowledge about the information asset, such as the legal department. The Information Security Officer (ISO)/designated security representative may also be called upon to advise and assist the information owner in determining the classification. A Trustee may add more questions, but may not alter or remove the original questions.
- f. Information assets are classified according to confidentiality, integrity, and availability. Each of these three principles of security is individually rated as low, moderate, or high. For example, an information asset may have a

confidentiality level of “high”, an integrity level of “moderate”, and an availability level of “low” (i.e., HML).

- g. Questions are categorized by confidentiality, integrity, and availability. If it is determined after answering a question that the rating for a security principle (e.g., confidentiality) is high, you are not required to complete the remaining questions in that category. However, doing so may provide you with a better understanding of the risks associated with the information asset. To save time, the questions at the beginning will typically help in determining whether the rating is high. Each question must be answered sequentially, to the best of the information owners’ abilities.

## 12. Determination of Controls

Once the information is classified, the classification can be used to determine appropriate controls. At a minimum, baseline controls shall be implemented. Additional controls may be placed on the information due to the source, or form it is in.

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. IT and Cybersecurity may amend its policies and standards at any time; compliance with amended policies and standards is expected.

## 13. Documentation

Trustees shall document, track, and report any approved variances or exceptions to the standards they established for their data. Any time there is a threat to the security of a Trustee’s appointed asset, they shall complete an Event and Audit Log not to be confused with the windows audit and event log (See Appendix “C”) and turn it into the Board of Trustees who shall review and evaluate with the IT&CS department for corrective action if it was system related. If it was staff related, it shall be brought to the attention of the Executive Director.

## 14. Consequences

Failure to follow these policies can result in the agency’s loss of integrity with the casinos and public. It can also result in litigation being filed against the agency, staff, and chain of command. Failure to follow these policies will result in disciplinary action handled in a progressive manner and on a case by case basis, up to and including dismissal of employment and filing of civil and criminal charges.

APPENDIX “A”  
DATA CLASSIFICATION WORK SHEET

Data Asset Evaluated: \_\_\_\_\_ Date: \_\_\_\_\_

Trustee: \_\_\_\_\_

Confidentiality Questions	
1.	Does the information include or contain PPSI (Personal, Private or Sensitive Information)?
A.	<b>No</b> – Continue with the Confidentiality questions
B.	<b>Unknown</b> – Confidentiality rating is High until the information is known (Rate Confidentiality High below and continue with integrity questions)
C.	<b>Possible</b> – Confidentiality rating is High until the information is known (Rate Confidentiality High below and continue with integrity questions)
D.	<b>Yes</b> – Confidentiality rating is High (rate below and continue with integrity questions)
2.	What impact does unauthorized access or disclosure of information have on health and safety?
A.	<b>None</b> – Continue with the Confidentiality questions
B.	<b>Limited impact</b> – Continue with the Confidentiality questions
C.	<b>Serious impact</b> – Continue with the Confidentiality questions
D.	<b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
3.	What is the financial impact of unauthorized access or disclosure of information?
A.	<b>None</b> – Continue with the Confidentiality questions
B.	<b>Limited impact</b> – Continue with the Confidentiality questions
C.	<b>Serious impact</b> – Continue with the Confidentiality questions
D.	<b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
4.	What impact does unauthorized access or disclosure of information have on the agency’s mission?
A.	<b>None</b> – Continue with the Confidentiality questions
B.	<b>Limited impact</b> – Continue with the Confidentiality questions
C.	<b>Serious impact</b> – Continue with the Confidentiality questions
D.	<b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
5.	What impact does unauthorized access or disclosure of information have on the public trust?
A.	<b>None</b> – Continue with the Confidentiality questions
B.	<b>Limited impact</b> – Continue with the Confidentiality questions
C.	<b>Serious impact</b> – Continue with the Confidentiality questions
D.	<b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)

6.	Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information.
A.	None – Continue with the Confidentiality questions
B.	Limited impact – Continue with the Confidentiality questions
C.	Serious impact – Continue with the Confidentiality questions
D.	Severe impact – Confidentiality rating is High (rate below and continue with integrity questions)
7.	Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure of information.
A.	None – Continue with the Confidentiality questions
B.	Limited impact – Continue with the Confidentiality questions
C.	Serious impact – Continue with the Confidentiality questions
D.	Severe impact – Confidentiality rating is High (rate below and continue with integrity questions)
8.	Is the information publicly available?
A.	No – See Instructions below, then continue with integrity questions
B.	Yes – See Instructions below, then continue with integrity questions
<p>If All of the above answers are A or B GREEN, rating is LOW; if ANY of the above answers are C YELLOW and None are D RED, rating is moderate; if ANY of the above answers are D (RED, rating is HIGH).</p>	

## Integrity Questions

1.	Does the information include medical records?
	<b>A.</b> No
	<b>B.</b> Unknown
	<b>C.</b> It could
	<b>D.</b> Yes
2.	Is the information (e.g., security logs) relied upon to make critical security decisions?
	<b>A.</b> No
	<b>B.</b> In the rarest of occasion
	<b>C.</b> They can be
	<b>D.</b> Yes
3.	What impact does unauthorized modification or destruction of information have on health and safety?
	<b>A.</b> <b>None</b> – Continue with the Confidentiality questions
	<b>B.</b> <b>Limited impact</b> – Continue with the Confidentiality questions
	<b>C.</b> <b>Serious impact</b> – Continue with the Confidentiality questions
	<b>D.</b> <b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
4.	What is the financial impact of unauthorized modification or destruction of information?
	<b>A.</b> <b>None</b> – Continue with the Confidentiality questions
	<b>B.</b> <b>Limited impact</b> – Continue with the Confidentiality questions
	<b>C.</b> <b>Serious impact</b> – Continue with the Confidentiality questions
	<b>D.</b> <b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
5.	What impact does the unauthorized modification or destruction of information have on KRGC's mission?
	<b>A.</b> <b>None</b> – Continue with the Confidentiality questions
	<b>B.</b> <b>Limited impact</b> – Continue with the Confidentiality questions
	<b>C.</b> <b>Serious impact</b> – Continue with the Confidentiality questions
	<b>D.</b> <b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
6.	What impact does unauthorized modification or destruction of information have on the public trust?
	<b>A.</b> <b>None</b> – Continue with the Confidentiality questions
	<b>B.</b> <b>Limited impact</b> – Continue with the Confidentiality questions
	<b>C.</b> <b>Serious impact</b> – Continue with the Confidentiality questions
	<b>D.</b> <b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
7.	Is integrity addressed by law or regulation? If yes, determine the impact of

	unauthorized modification or destruction of information.
A.	None – Continue with the Confidentiality questions
B.	Limited impact – Continue with the Confidentiality questions
C.	Serious impact – Continue with the Confidentiality questions
D.	Severe impact – Confidentiality rating is High (rate below and continue with integrity questions)
8.	Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information.
A.	No – See Instructions below then continue with Availability questions
B.	Yes - Limited impact – see Instructions below then continue with Availability questions.
C.	Yes – Serious impact – See instructions below then continue with Availability questions.
D.	Yes – Severe impact – Integrity is High(Rate Below), continue with Availability questions.
If All of the above answers are A or B GREEN, rating is LOW; if ANY of the above answers are C YELLOW and None are D RED, rating is moderate; if ANY of the above answers are D (RED, rating is HIGH).	

### Availability Questions

1.	Is availability of the information essential for emergency response or disaster recovery?
	<b>A.</b> No – Continue with availability questions
	<b>B.</b> Yes – Availability is High (Rate Below)
2.	This information needs to be provided or available:
	<b>A.</b> As time permits – Continue with Availability questions
	<b>B.</b> Within 1 to 7 days – continue with Availability questions
	<b>C.</b> Unknown – Availability is High (rate below)
	<b>D.</b> 24 hrs. per day/7 days a week – Availability is High (rate below)
3.	What is the impact to health and safety if information were not available when needed?
	<b>A.</b> None – Continue with the Availability questions
	<b>B.</b> Limited impact – Continue with the Availability questions
	<b>C.</b> Serious impact – Continue with the Availability questions
	<b>D.</b> Severe impact – Confidentiality rating is High (rate below and continue with Availability questions)
4.	What is the financial impact if information were not available when needed?
	<b>A.</b> None – Continue with the Availability questions
	<b>B.</b> Limited impact – Continue with the Availability questions
	<b>C.</b> Serious impact – Continue with the Availability questions
	<b>D.</b> Severe impact – Confidentiality rating is High (rate below and continue with Availability questions)
5.	What is the impact to the KRGC mission if information were not available when needed?
	<b>A.</b> None – Continue with the Availability questions
	<b>B.</b> Limited impact – Continue with the Availability questions
	<b>C.</b> Serious impact – Continue with the Availability questions
	<b>D.</b> Severe impact – Confidentiality rating is High (rate below and continue with Availability questions)
6.	What is the impact to the public trust if the information were not available when needed?
	<b>A.</b> None – See instructions below
	<b>B.</b> Limited impact – Continue with the Availability questions
	<b>C.</b> Serious impact – Continue with the Availability questions
	<b>D.</b> Severe impact – Confidentiality rating is High (rate below and continue with Availability questions)
<p>If All of the above answers are <b>A or B GREEN</b>, rating is <b>LOW</b>; if ANY of the above answers are <b>C YELLOW</b> and None are <b>D RED</b>, rating is moderate; if ANY of the above answers are <b>D (RED, rating is HIGH)</b>.</p>	

**APPENDIX “B”  
INSTRUCTIONS ON DATA INFORMATION WORK SHEET**

<b>Confidentiality Questions</b>	
1.	Does the information include or contain PPSI (Personal, Private or Sensitive Information)?
<b>A.</b>	<b>None</b> – Continue with the Confidentiality questions
<b>B.</b>	<b>Unknown</b> – Confidentiality rating is High until the information is known (Rate Confidentiality High below and continue with integrity questions)
<b>C.</b>	<b>Possible</b> – Confidentiality rating is High until the information is known (Rate Confidentiality High below and continue with integrity questions)
<b>D.</b>	<b>Yes</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	Example(s): A W-2 form contains a name, as well as a social security number. This would be considered private information and therefore have a confidentiality of high. The same is true with backgrounds, and what do they contain that would fall into this category, particularly on backgrounds where we recommend an individual not receive a license.
2	What impact does unauthorized access or disclosure of information have on health and safety?
<b>A.</b>	<b>None</b> – Continue with the Confidentiality questions
<b>B.</b>	<b>Limited impact</b> – Continue with the Confidentiality questions
<b>C.</b>	<b>Serious impact</b> – Continue with the Confidentiality questions
<b>D.</b>	<b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	Example(s): There may be information which, if publicly released, may impact the health and safety of KRGC and Kansas citizens. For instance, the blueprint and drawings of critical infrastructure buildings, critical infrastructure related systems and network configurations, and disaster recovery/business continuity plans could be exploited by criminals to sabotage or destroy buildings, emergency services, and critical infrastructure operations resulting in a severe impact thereby placing these items in the high confidentiality category.
3.	What is the financial impact of unauthorized access or disclosure of information?
<b>A.</b>	<b>None</b> – Continue with the Confidentiality questions
<b>B.</b>	<b>Limited impact</b> – Continue with the Confidentiality questions
<b>C.</b>	<b>Serious impact</b> – Continue with the Confidentiality questions
<b>D.</b>	<b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	Example(s): The KRGC may be exposed to litigation or regulatory fines due to disclosure of information protected by confidentiality agreements. For instance, unauthorized release of vendor bid information before the final submission date could jeopardize the bidding process leading to litigation.

		Similarly, if the investment decisions of a retirement system become known prior to their execution, it could alter the market sentiment ahead of the investment causing financial losses.
4.	What impact does unauthorized access or disclosure of information have on the agency's mission?	
	A.	None – Continue with the Confidentiality questions
	B.	Limited impact – Continue with the Confidentiality questions
	C.	Serious impact – Continue with the Confidentiality questions
	D.	Severe impact – Confidentiality rating is High (rate below and continue with integrity questions)
	<p>Example(s): An agency may be charged with ensuring that illegal goods do not enter State borders. As part of that mission, the agency may be responsible for collecting information regarding unmanned border crossings. If there was an unauthorized release of that information, resulting in an increase of illegal traffic across State borders, it could have a severe impact on the agency's ability to conduct its mission.</p> <p>An example of limited impact would be the release of employee contact information which may result in additional phone calls/emails/office visits.</p> <p>If a list of local delivery restaurants and their phone numbers is disclosed, there would be no impact.</p>	
5.	What impact does unauthorized access or disclosure of information have on the public trust?	
	A.	None – Continue with the Confidentiality questions
	B.	Limited impact – Continue with the Confidentiality questions
	C.	Serious impact – Continue with the Confidentiality questions
	D.	Severe impact – Confidentiality rating is High (rate below and continue with integrity questions)
	<p><b>Example(s):</b> It is important for the government to maintain the public's trust. Any breach of confidentiality that violates the public trust would typically lead to a severe impact for the agency. For example, the exposure of confidential medical records via a security breach could lead to a loss of public trust.</p> <p>A department which collects and maintains the confidential records of citizens requires a high level of trust from the public. Disclosure of data through a malicious insider, external hacker, or through a random accident could erode trust leading to political consequences for department management and for the State as a whole.</p>	
6.	Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information.	
	A.	None – Continue with the Confidentiality questions
	B.	Limited impact – Continue with the Confidentiality questions
	C.	Serious impact – Continue with the Confidentiality questions

	<b>D. Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	Example(s): Some types of information, including personal health records, student grades, and financial and personnel records may be protected by Federal, State, and local laws. Disclosing this information can lead to civil or criminal liability. There are several key statutes, such as HIPAA, that should be examined based on the information asset being classified.
7.	Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure of information.
	<b>A. None</b> – Continue with the Confidentiality questions
	<b>B. Limited impact</b> – Continue with the Confidentiality questions
	<b>C. Serious impact</b> – Continue with the Confidentiality questions
	<b>D. Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	<p><b>Example(s):</b> Some information generated within KRGC is for internal use only and is not meant to be disclosed externally. The confidentiality of such information varies considerably based on the information asset. Information, such as system security configurations, which, if released, could jeopardize the security of an agency’s assets, would require high confidentiality controls.</p> <p>Administrative information, such as procedures for travel approval, though not publicized outside the agency, would be information that the public could legitimately obtain and should be ranked as low in confidentiality.</p>
8.	Is the information publicly available?
	<b>A. No</b> – See Instructions below, then continue with integrity questions
	<b>B. Yes</b> – See Instructions below, then continue with integrity questions
	<p><b>Example(s):</b> Information that must be lawfully made available to the general public from Federal, State, or local government records or any information that does not need to be withheld for security or privacy concerns is generally public. Examples include public transportation schedules, a listing of local city events and health improvement guidelines. These items would be ranked low in confidentiality.</p>
	If All of the above answers are <b>A or B GREEN</b> , rating is <b>LOW</b> ; if ANY of the above answers are <b>C YELLOW</b> and None are <b>D RED</b> , rating is moderate; if ANY of the above answers are <b>D (RED, rating is HIGH)</b> .

## Integrity Questions

1.	Does the information include medical records?	
	<b>A.</b>	No
	<b>B.</b>	Unknown
	<b>C.</b>	
	<b>D.</b>	Yes
<p><b>Example(s):</b> In the case of a health care institution, it is important that medical records and medical history are accurate. For example, it may be important to know whether someone is allergic to specific medications so that they are not administered. In addition, it would be necessary to know whether a person has a particular illness or medical condition which would require special treatment. Malicious alteration to such records in medical institutions can cause serious health consequences for the patients.</p> <p style="text-align: center;">Medical records require high integrity.</p>		
2	Is the information (e.g., security logs) relied upon to make critical security decisions?	
	<b>A.</b>	No
	<b>B.</b>	
	<b>C.</b>	
	<b>D.</b>	No
<p><b>Example(s):</b> It is important that security records (e.g., computer security logs, building security access logs) are accurate in order to verify legitimate access and identify unauthorized access attempts. Security records require high integrity.</p>		
3.	What impact does unauthorized modification or destruction of information have on health and safety?	
	<b>A.</b>	<b>None</b> – Continue with the Confidentiality questions
	<b>B.</b>	<b>Limited impact</b> – Continue with the Confidentiality questions
	<b>C.</b>	<b>Serious impact</b> – Continue with the Confidentiality questions
	<b>D.</b>	<b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
<p><b>Example(s):</b> There is a potential for severe impact on the safety of citizens if someone accesses an airline system and modifies the onboard navigation system.</p> <p style="text-align: center;">The removal or editing of surveillance tapes may have a serious or severe impact depending on the presence of other information provided by surveillance.</p> <p style="text-align: center;">Something that could be of limited to no impact on health and safety would be the modification of employee calendars.</p>		

4.	What is the financial impact of unauthorized modification or destruction of information?
	A. <b>None</b> – Continue with the Confidentiality questions
	B. <b>Limited impact</b> – Continue with the Confidentiality questions
	C. <b>Serious impact</b> – Continue with the Confidentiality questions
	D. <b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	Example(s): There are many financial implications for the destruction or modification of information. It does not strictly mean monetary loss, but can also indicate loss of employee time and effort for recovery. Something that would have severe financial impact might be the loss of all financial records from KRGC's financial management database.
5.	What impact does the unauthorized modification or destruction of information have on the agency mission?
	A. <b>None</b> – Continue with the Confidentiality questions
	B. <b>Limited impact</b> – Continue with the Confidentiality questions
	C. <b>Serious impact</b> – Continue with the Confidentiality questions
	D. <b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	Example(s): Agency operations could be drastically affected if information is changed without authorization. For example, if someone removed all the phone numbers in a Do Not Call registry, it would severely impact the mission of the program to prevent unwanted calls to registered numbers.  The mission of this agency is to investigate and certify the qualifications of casino staff employee applicants and vendors through background investigations. Malicious or accidental changes to those records would have a severe impact on the agency's mission.
6.	What impact does unauthorized modification or destruction of information have on the public trust?
	A. <b>None</b> – Continue with the Confidentiality questions
	B. <b>Limited impact</b> – Continue with the Confidentiality questions
	C. <b>Serious impact</b> – Continue with the Confidentiality questions
	D. <b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	Example(s): The public relies on government to provide accurate information. Failure to do so would erode public trust. For example, if information on certification for licensing was inaccurately modified without authorization and then posted to a public web site, the public would no longer trust the posting as a reputable source for this information.
7.	Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.
	A. <b>None</b> – Continue with the Confidentiality questions
	B. <b>Limited impact</b> – Continue with the Confidentiality questions

	<b>C.</b> <b>Serious impact</b> – Continue with the Confidentiality questions
	<b>D.</b> <b>Severe impact</b> – Confidentiality rating is High (rate below and continue with integrity questions)
	Example(s): Some types of information, including personal health records, student grades, and financial and personnel records, may be protected by Federal, State, and local laws. Allowing unauthorized changes to information may have legal consequences. There are several key statutes that should be examined based on the information asset being classified. For example, HIPAA requires safeguards to protect against threats to the integrity of electronic protected information.
8.	Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information.
	<b>A.</b> <b>No</b> – See Instructions below then continue with Availability questions
	<b>B.</b> <b>Yes - Limited impact</b> – see Instructions below then continue with Availability questions.
	<b>C.</b> <b>Yes</b> – Serious impact – See instructions below then continue with Availability questions.
	<b>D.</b> <b>Yes – Severe impact</b> – Integrity is High(Rate Below), continue with Availability questions.
	Example(s): It is important for financial information to remain reliable. Unauthorized changes to financial transactions (e.g., direct deposit, electronic funds transfer) could severely impact the financial stability of the agency.  Employee appraisal records are used to make important personnel decisions. Someone may attempt to falsify records in hopes of getting a promotion, alternate employment or to diminish someone else’s reputation and/or record. The impact to the agency could vary dependent upon the situation.
	If All of the above answers are <b>A or B GREEN</b> , rating is <b>LOW</b> ; if ANY of the above answers are <b>C YELLOW</b> and None are <b>D RED</b> , rating is moderate; if ANY of the above answers are <b>D (RED, rating is HIGH)</b> .

### Availability Questions

1.	Is availability of the information essential for emergency response or disaster recovery?		<p><b>A. No</b> – Continue with availability questions</p> <p><b>B. Yes</b> – Availability is High (Rate Below)</p>
			<p>Example(s): If the information asset is required for emergency response, it could be essential in saving lives or in coordinating law enforcement and health officials during an emergency or disaster. Therefore, it must be available upon immediate request (high availability).</p> <p>Disaster Recovery Plans need to be available in case of emergencies. Although required infrequently, they have a high availability status.</p>
2.	This information needs to be provided or available:		<p><b>A. As time permits</b> – Continue with Availability questions</p> <p><b>B. Within 1 to 7 days</b> – continue with Availability questions</p> <p><b>C. Unknown</b> – Availability is High (rate below)</p> <p><b>D. 24 hrs. per day/7 days a week</b> – Availability is High (rate below)</p>
			<p>Example(s): Intrusion detection systems send event notifications so that an incident can be analyzed and escalated based on the level of threat. Since security is critical, and severe damage can be caused to KRGC data and networks, this operation is time critical and requires high availability.</p>
3.	What is the impact to health and safety if information were not available when needed?		<p><b>A. None</b> – Continue with the Availability questions</p> <p><b>B. Limited impact</b> – Continue with the Availability questions</p> <p><b>C. Serious impact</b> – Continue with the Availability questions</p> <p><b>D. Severe impact</b> – Confidentiality rating is High (rate below and continue with Availability questions)</p>
			<p>Example(s): Medical records contain information (e.g., allergies, blood type, previous medications) which is critical for providing patients with accurate medical care. Lack of availability to this data during emergency medical care can lead to life threatening situations therefore placing these items in the high availability category.</p>
4.	What is the financial impact if information were not available when needed?		<p><b>A. None</b> – Continue with the Availability questions</p> <p><b>B. Limited impact</b> – Continue with the Availability questions</p> <p><b>C. Serious impact</b> – Continue with the Availability questions</p> <p><b>D. Severe impact</b> – Confidentiality rating is High (rate below and continue with Availability questions)</p>
			<p>Example(s): For any agency that does not generate revenue, a disruption of service can have a limited financial impact which could be deemed minor.</p> <p>A personal computer system crash which can be solved by a simple reboot would have limited impact.</p>

5.	What is the impact to the KRGC mission if information were not available when needed?
A.	None – Continue with the Availability questions
B.	Limited impact – Continue with the Availability questions
C.	Serious impact – Continue with the Availability questions
D.	Severe impact – Confidentiality rating is High (rate below and continue with Availability questions)
	Example(s): How would it be received if we needed to contact the casinos and advise them we lost the data requested in this case is not available at this time?
6.	What is the impact to the public trust if the information were not available when needed?
A.	None – See instructions below
B.	Limited impact – Continue with the Availability questions
C.	Serious impact – Continue with the Availability questions
D.	Severe impact – Confidentiality rating is High (rate below and continue with Availability questions)
	Example(s): KRGC has spent considerable effort modernizing operations to include online services and encouraging the vendors and applicants to use these services. If these services are seriously degraded or disrupted, this could cause serious embarrassment to KRGC resulting in a severe impact. The availability in this case would be high.
<p>If All of the above answers are A or B GREEN, rating is LOW; if ANY of the above answers are C YELLOW and None are D RED, rating is moderate; if ANY of the above answers are D (RED, rating is HIGH.</p>	

**APPENDIX “C”  
INACT LEVEL CONSIDERATIONS**

Using the Cybersecurity triad of confidentiality, Integrity, and availability, each Trustee of data shall review the impact levels in the context of its own operational environment. Figure 1 below demonstrates the *Information Asset Classification Matrix*.

	<b>INFORMATION CLASSIFICATION CATEGORIES</b>		
	<b>LOW</b>	<b>MODERATE</b>	<b>HIGH</b>
<p><b>CONFIDENTIALITY</b> Consider impact of unauthorized disclosure on factors such as:</p> <ul style="list-style-type: none"> <li>• Health and Safety</li> <li>• Financial Loss</li> <li>• Agency Mission/Programs</li> <li>• Public Trust</li> </ul>	The unauthorized access or disclosure of information would have <b><i>limited or no impact</i></b> to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of information would have <b><i>serious impact</i></b> to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of PPSI or other information would have a <b><i>severe or catastrophic impact</i></b> on the organization, its critical functions, workforce, business partners and/or its customers.
<p><b>INTEGRITY</b> Consider impact of unauthorized modification or destruction on factors such as:</p> <ul style="list-style-type: none"> <li>• Health and Safety</li> <li>• Financial Loss</li> <li>• Agency Mission/Programs</li> <li>• Public Trust</li> </ul>	The unauthorized modification or destruction of information would have <b><i>limited or no impact</i></b> to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have <b><i>serious impact</i></b> to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have a <b><i>severe or catastrophic impact</i></b> on the organization, its critical functions, workforce, business partners and/or its customers.
<p><b>AVAILABILITY</b> Consider impact of untimely or unreliable access to information on factors such as:</p> <ul style="list-style-type: none"> <li>• Health and Safety</li> <li>• Financial Loss</li> <li>• Agency workflow</li> <li>• Mission/Programs</li> <li>• Public Trust</li> </ul>	The disruption of access to or use of information would have <b><i>limited or no impact</i></b> to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have <b><i>serious impact</i></b> to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have a <b><i>severe or catastrophic impact</i></b> on the organization, its critical functions, workforce, business partners and/or its customers.
Information Asset Classification Matrix - based on the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems			

APPENDIX "D"

AUDIT AND EVENT LOG

REPORTING PARTY: \_\_\_\_\_ DATE: \_\_\_\_\_

TIME AND DATE OF EVENT: TIME: \_\_\_\_\_ DATE: \_\_\_\_\_

**NATURE OF EVENT:**

SYSTEM RELATED:  IMMEDIATELY REPORTED TO IT? YES  NO

STAFF RELATED:

**LEVEL OF CONCERN:**

LIMITED IMPACT

SERIOUS IMPACT

SEVERE IMPACT

**BRIEF SYNOPSIS OF EVENT:**


**CORRECTIVE ACTION AT TIME**


**CYBERSECURITY POLICY  
ASSESSMENT AND SECURITY PLANNING**

**Number Draft #3  
2020-07**

<b>Adopted</b> September 11, 2020	<b>Last Revision</b>	<b>Rescinds</b> Any previous IT policies
<b>Commission Authorization</b>		
<b>Chairman Brandon Jones</b>	<b>Date</b>	

**I. Purpose/Background**

This policy is promulgated pursuant to the Kansas Cybersecurity Act of 2018, K.S.A. 2018 Supp. 75-7236 through 75-7243, and amendments thereto which caused the generation of ITEC 7230A mandating controls on executive agencies to address cybersecurity issues. In §7.1, it required this agency to assess and document the risks to Information Systems that store or transmit “Restricted-Use Information” and assess potential threats and characteristics and the likelihood and impact of these threats.

**II. Introduction**

KRGC receives, stores, and transmits a multitude of data that is required to be addressed as Personal Identifiable Information (PII). Under §7.0 of ITEC7230A, KRGC is required to assess the risks that accompany these task.

**III. Policy**

Annually, KRGC IT&CS with the Board of Trustees shall meet to assess and document the risks to Information Systems that process, store or transmit Restricted-Use Information and, in completing this task, shall identify the vulnerabilities and related threats. The standing vulnerabilities and threats are in section III.A. and III.B. This shall entail assessments of any reported activity, responses to incidents, and other concerns observed.

**A. Identified Vulnerabilities**

Threats and concerns will be identified in the following manners. The internal problems will be considered vulnerabilities, the abilities to cause a problem from the outside the system are considered threats. KRGC is not able to address external threats, so the focus of the plan is on their vulnerabilities. With that consideration, and attempting to maintain a layered cybersecurity approach, the evaluation is broken down into the following:

1. People
  - a. Training
  - b. Assignment of duties
  - c. Strong Passwords
  - d. Restraints on Phishing attacks
  - e. Reporting system for suspected abuse, intrusion, attempts, or unusual activity on their computer.
  - f. Adequate access controls.
  - g. Desire for ease of use.
2. People Corrective Processes
  - a. Training
  - b. Established Standard Operational Procedures
  - c. Sensitive information
  - d. Establishing ownership of the data
3. Technology
  - a. Tools to prevent Incident prevention and Incident Detection
  - b. Tools for recovery
  - c. Adequate firewalls
  - d. System backup
  - e. Method of encryption (in transit and at rest)
4. Incident prevention
  - a. Business Continuity Plan
  - b. Disaster Recovery Plan

- c. Incident Response plan
- d. Patch program
- e. Regular Cybersecurity evaluation
- f. Prioritization of assets
- g. Adequately encrypting

#### **IV. Threats**

##### **A. Employees**

Employees are one of the biggest security threats. They may do damage to the systems either through incompetence or intentionally.

##### **B. Amateur Hackers and Vandals**

Except through spam and phishing, the probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network. Amateurs have a goal. Amateurs think they are good at everything.

##### **C. Professional Criminal Hackers and Saboteurs**

Professionals have a proven process which makes them money, and they may be hired by corporations or governments. Professionals understand their circles of competence and focus on that area. Professionals understand that the initial achievement is just the beginning. The probability of this type of attack is low, but not completely unlikely, due to the amount of sensitive information contained in KRGC databases.

#### **V. Assessment**

KRGC shall use the elements of items III and IV to assess the risk to the network that processes, stores, or transmits the restricted-use information at all KRGC properties. The evaluation will be done on all three levels of people, process, and technology to prevent the three threats of employee, amateur and professional hackers from maximizing on those threats. The belief is that the system is as strong as the cybersecurity at the weakest property.

- A. This assessment will also be done prior to any major change to the system, evaluating the need for the change and the effect it will have on the system's cybersecurity.

- B. The process will be repeated every three (3) years thereafter.
- C. A report of the problems discovered, with recommendations will be prepared and presented by the Information Technology and Cybersecurity unit to the Executive Director.
  - 1. If equipment is recommended, it will include cost assessments.
  - 2. It will also advise how much of these services can be received within the state system.

## **VI. Risk Assessment and Security Planning**

Based on the finding of the cybersecurity assessment, KRGC shall review the current cybersecurity plan, including training, program, and equipment needs, and make adjustments to address the deficiencies found in the assessment for any Information Systems that process, store or transmit Restricted-Use Information.

## **VII. Post Corrective Action**

Within 60 days, and on completion of the corrections, KRGC Information Technology and Cybersecurity shall conduct another assessment to determine if the corrections, did adequately mitigate the risks. Any corrective action concerns shall be immediately be brought to the attention of the executive director.

<b>Subject</b>	<b>Number</b>	<b>Draft #</b>
<b>CYBERSECURITY POLICY                  AWARENESS AND TRAINING</b>	<b>2020-08</b>	<b>(3)</b>

<b>Adopted</b> September 11, 2020	<b>Last Revision</b>	<b>Rescinds</b>
--------------------------------------	----------------------	-----------------

<b>Commission Authorization</b>	
---------------------------------	--

Chairman Brandon Jones	Date
------------------------	------

**I. Purpose/Background**

This policy is promulgated pursuant to the Kansas cybersecurity act, K.S.A. 2018 Supp. 75-7236 through 75-7243, and amendments thereto. It is specifically designed to meet the requirements of section 8.0 (Awareness and Training Standard) of the ITEC 7230A publication, and is one part of the KRGC’s overall Cybersecurity Policy.

**II. Introduction**

- A. Training of staff, the Information Technology Team, and the Cybersecurity team is paramount to developing a sound, ongoing cybersecurity program. This policy addresses how KRGC reaches this goal for new and current staff.
- B. The policy covers training new hires, the second annual training, training on demand, and a Test, Training, and Exercise program to ensure peak performance of employees as well as to trouble shoot system safeguards and procedures. The Test portion of the program could indicate written exams or simply reviews, but will also test the methods and the equipment used.

**III. Policy**

- A. A major threat to the agency’s Cyber Structure is its employees. The best way to combat this threat is through both initial and ongoing training. These standards and training are mandatory for all agency employees and commissioners. All users are required to receive Information Technology Awareness training on initial hire and annually thereafter. New hires will be given training within 90 days of their initial hire. Related training will be provided annually for all employees by the Information Technology and Cybersecurity Unit. After the initial hire training and any annual training, the participants will sign a statement (See Appendix “A”) advising they participated in and understand the training, as well as KRGC regulations on the issues

of KRGC Cybersecurity. The KRGC Training Manager is responsible for conducting the training, and support for that training will be provided by the IT&CS Department. Support can include, but not be limited to, PowerPoint development, demonstration of training materials, or tutoring.

- B. Initial training will contain the following subjects and shall be conducted within 90 days of hiring. At a minimum, the training will be sufficient to provide two (2) hours of CEUs to a law enforcement officer at the Kansas CPOST. The subject material shall include the following:
  - 1. Passwords, including creation, changing, aging, and confidentiality
  - 2. Privacy and proper handling of sensitive information
  - 3. Physical security
  - 4. Social engineering
  - 5. Identity theft avoidance and action
  - 6. Email usage
  - 7. Internet usage
  - 8. Viruses and malware
  - 9. Software usage, copyrights, and file sharing
  - 10. Portable electronic devices and portable electronic media
  - 11. Proper use of encryption devices
  - 12. Reporting of suspicious activity and abuse
  
- C. All KRGC staff and any authorized user of the KRGC IT system shall receive annual training. At a minimum, the training will be sufficient to provide two (2) hours of CEUs to a law enforcement officer at the Kansas CPOST, and will consist of a refresher on the topics listed in III.B as well as:
  - 1. New known methods of phishing, spam, and social engineering
  - 2. Latest news in hacking and computer crime
  
- D. Training on demand

1. KRGC staff will also receive one-on-one training on demand. The demand will be determined based on that staff member's violation of the Cybersecurity regulations or succumbing to social engineering ruses such as phishing attempts.
  2. KRGC will conduct penetration tests that include elements of social engineering. An individual who inadvertently permits an attempt to be successful will receive immediate training in order to reinforce the correct response to a social engineering attempt. For example, a penetration test may include a phishing attempt. If the employee responds to the phishing email by clicking on the included URL link, the link will take them to an immediate training exercise.
  3. Training shall be of quality to meet continuing education requirements for the agency Law Enforcement staff under K.S.A. 74-5607a and 74-5604a.
- E. KRGC shall conduct a Test, Training, and Exercise Program based on the NIST Special Publication 800-84 (*Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*). This will test the effectiveness of the agency's cybersecurity program and meet the needs for classroom and tabletop exercises under ITEC7230 §15.7.
1. Tabletop exercises will be conducted as part of the Test, Training, and Exercise program. Tabletop exercises are discussion-based events where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. Tabletop exercises are conducted in an informal environment, with a facilitator guiding participants through a discussion designed to meet pre-defined objectives. Planning and performing tabletop exercise events has the following phases:
    - a. Assess Needs

Prior to developing an exercise, KRGC IT and Training shall first conduct a needs assessment to define the problems and concerns that will be addressed in the exercise. This will include consideration of functions that need to be exercised, including areas of vulnerability, functions in need of rehearsal, and areas found needing improvement in past exercises.
    - b. Define the Scope

To provide better focus, the boundaries and scope of the exercise shall be determined in identifying where the activity will take place. Elements considered and included will be the type of emergency, the areas or locations where the simulated event will occur, the type of functions the participants will take during the exercise, and the specific list of intended participants.
    - c. Purpose Statement

The training plan will include the purpose of the exercise. It will facilitate the selection of the objectives and clarify why the exercise subject is selected.

d. Define the Objectives

Well-defined objectives provide a framework for scenario development, guide individual organizations' objective development, inform exercise evaluation criteria, and synchronize various agencies' efforts towards common goals to prevent duplication of effort and focus support on exercise priorities.

Generally, planners should limit the number of exercise objectives to enable timely exercise conduct, facilitate reasonable scenario design, and support successful completion of exercise goals. Capabilities, tasks, and objectives are initially prepared during a Concept and Objectives (C&O) Meeting or Initial Planning Meeting (IPM).

e. Development of Scenario

An outline or model of the simulated sequence of events for the exercise which provides the backdrop that drives participant discussion will be included in the tabletop exercise. The planner should develop scenarios which enable an exercise to meet its objectives. The scenario shall be realistic, plausible, and challenging.

For all scenarios, the date and time affect exercise play. Many communities have different population demographics on weekdays, weekends, and holidays, as well as at night and during special events. These changes may affect players' expected actions and can be incorporated into the scenario. For example, the IT department is not a 24/7 operation. A scenario that occurs after hours could change the actions that would take place.

f. Determination of the key factors

Major and detailed events are occurrences, both large and small, that take place after and as a result of the emergency described in the scenario. The goal in developing these events is to provide a structure that will link the simulated event to the actions that will exercise player's abilities and considerations.

Major events are big problems resulting from the event. They should be likely events that require realistic action. To arrive at a list of major events, it is important to first identify several major occurrences that might follow the event, and then to decide which of these events might generate situations that would test the objectives.

Detailed events are specific problem situations to which personnel must respond. Each detailed event should be designed to prompt one or more expected actions for one or more organizations that are participating in the exercise.

g. Post training de-briefing

After every exercise, there shall be a debriefing and discussion. The planner should have a list of the major and detailed events that have been identified, and develop discussion questions that can be presented at the tabletop exercise.

Discussion questions should prompt players to address specific problems or issues that link back to the exercise objectives. Depending on the length, scope, and complexity of your exercise scenario and major/detailed events, the exercise scenario and associated questions may be presented to players in one, two, or three distinct time modules to allow for in-depth discussion for different phases of the event response.

2. Frequency of Tabletop exercises

At a minimum, KRGC IT and Cybersecurity unit with the Executive Staff shall conduct a tabletop exercise once each calendar year. Tabletop exercises will also be conducted following organizational changes, updates to an IT plan, or the issuance of new TT&E guidance; or as otherwise needed.

3. Objective of an exercise

The objectives of any tabletop exercise should be validating the content and needs of the IT plan and related policies and procedures, validating participants' roles and responsibilities as documented in the plan, and validating the interdependencies documented in the plan.

4. Topics and Structure

The staff will use the KRGC Cybersecurity training handbook to guide them through the execution of a tabletop exercise. The subject shall be selected by the Director of Information Technology and Cybersecurity.

5. Topic

IT and Cybersecurity should determine the exercise topic based on the focus of the plan being exercised. General topics can include contingency planning and incident response. Specific topics range from sustaining essential functions to managing and reporting IT security incidents. For example, disaster recovery plan exercise discussion topics would likely include the roles and responsibilities of personnel

with regard to the processes and procedures associated with restoring an organization's information systems. Incident response plan exercise discussion topics would likely include processes and procedures for managing and reporting IT security incidents.

#### 6. Functional Exercise

In lieu of a tabletop exercise, the staff may also conduct a Functional Exercise. The functional exercise shall be held under as much scrutiny as the tabletop exercise. See the training manual for details on this type of exercise.

#### 7. Debriefing

There shall be a debriefing immediately following a tabletop or functional exercise (no later than the following work day). A report from the debriefing shall be made and submitted to the executive staff.

#### 8. Annual training

Independent of the tabletop or functional exercise training, the C-SIRT members shall receive forty (40) hours of IT and Cybersecurity training. The training shall be sufficient to provide forty (40) hours of CEUs to a law enforcement officer at the Kansas CPOST.

### F. IT and Cybersecurity Staff training

The Information Technology and Cybersecurity security staff are all part of the Cybersecurity Incident Response Team for the agency and require additional training. Within the first year, all members of the team shall be trained as Systems Security Certified Practitioners (SSCP). This trains them in the following seven (7) security domains under the Common Body of Knowledge (CBK):

1. Introducing Security and Aligning Asset Management to Risk Management
2. Understanding Risk Management Options and the Use of Access Controls to Protect Assets
3. Cryptography
4. Securing Software, Using Security Protocols and Securing Remote Users
5. Networking
6. Security Testing and Incident Handling
7. Physical Security, Managing Change and Personnel Training

G. Annually, at a minimum, the agency shall train the IT and Cybersecurity staff to maintain their knowledge of Systems Security Certified Practitioner certificate, and certification should they have any certifications requiring annual training (e.g., SSCP would require a minimum of 40 hours of related training in the seven (7) domains for continued certification).

APPENDIX "A"

STATEMENT OF UNDERSTANDING FOR  
INFORMATION TECHNOLOGY STANDARDS

I, \_\_\_\_\_, have been provided training and information on the Information Technology standards for the Kansas Racing and Gaming Commission. I understand as a user I must follow these standards, and failure to do so could result in disciplinary action up to, and including, dismissal. I have also read and understand the specific regulations and controls listed below:

1. I understand I must complete cybersecurity training in the next 90 days, followed by annual training pertaining to the same subject.
2. I must change my password every ninety (90) days, it must be fifteen (15) characters in length containing capital letters, small case letters, numbers, and special characters in the same password.
3. I am solely responsible for the security of my passwords, and will not share them, or jeopardize their security. I will not share my password with anyone, to include my supervisor.
4. I will not use the same system password for any other password.
5. Use of the internet on the KRGC system is for business purposes only.
6. I understand I must repeat cybersecurity awareness training annually as directed.
7. I understand I am responsible for any Information Technology Equipment assigned to me, any loss or damage caused by could result in disciplinary action up to and including dismissal.
8. I will report any suspected system breaches or attempts, including those used by phishing, to the KRGC Information Technology and Cybersecurity Department as soon as possible.
9. I will follow all the regulations in the KRGC Cybersecurity policy 2020-01 and its sub-components.

I have read and understand the previous nine (9) listed conditions above and agree to comply with them, understanding that failure to do so could result in disciplinary action up to and including my discharge from this agency.

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

Witness: \_\_\_\_\_ Date: \_\_\_\_\_

<b>Subject</b>		<b>Number</b>	<b>Draft #</b>
<b>CYBERSECURITY POLICY ACCESS CONTROL</b>		<b>2020-09</b>	<b>(3)</b>
<b>Adopted</b>	<b>Last Revision</b>	<b>Rescinds</b>	
September 11, 2020		Any previous IT policies	
<b>Commission Authorization</b>			
Chairman Brandon Jones	Date		

**I. Purpose/Background**

This policy is promulgated pursuant to the Kansas Cybersecurity Act of 2018, K.S.A. 2018 Supp. 75-7236 through 75-7243, and amendments thereto which caused the generation of ITEC 7230A mandating controls on executive agencies to address cybersecurity issues. Section 7.1 of the act requires this agency to assess and document the risks to Information Systems that store or transmit, “Restricted-Use Information”, including an assessment of the potential threats and characteristics with the likelihood and impact of these threats.

**II. Introduction**

KRGC receives, stores, and transmits a multitude of data that is required to be addressed as Personal Identifiable Information (PII). Therefore, it is required to assess the risks that accompany this task. Under Section 9.0 of ITEC7230A, the agency is required to maintain minimum access control standards.

**III. Policy**

A. Authentication

KRGC’s system handles the access to Critical Systems and Information Systems that process, store or transmit Restricted-Use Information; therefore, they shall be authorized by an appropriate Entity official through established protocols within the agency.

1. Data Trustee

There shall be a Data Trustee assigned to all data in the system, and the trustee shall be the owner of data as it is being developed, collected, stored, and transmitted.

The Data Trustee shall have the authority to determine who has access to this system, either while the information is in its formative state, or in the final state.

Before a user of this data is granted access, the IT&CS department shall receive authority for the user to access the data from both the user's supervisor and the data's Data Trustee. Either may place restrictions on that access and the most restrictive instructions shall be followed.

2. All users shall be provided a unique identifier

Each user shall be provided a sign-in and the ability to have a password, with a "token" for one time passwords that allow the use to gain access to the system. There shall be no repeat of identifiers.

3. Administrative privileges

Users with administrative rights or elevated privileges shall use a separate account to perform tasks that require elevated privileges or administrative rights. They shall use the password for that account and their own token for two-factor authentication.

Administrative user accounts shall only be used for activities that require elevated privileges (i.e. not for email access or internet browsing) and shall require two-factor authentication for their use, Administrative accounts shall not have an assigned email account or mailbox.

4. System Service Accounts

System Service Accounts are unique accounts that an application or service uses to interact with the operating system. Services may use the system service account to log on and make changes to the operating system or the configuration. Each system service account shall be approved and documented for proper business use by either the Director of IT&CS or the Network Specialist and shall be reviewed and approved annually for continued use. These accounts will be configured with minimal privileges and only used for a single task or service. The unique system identifiers shall be associated with a unique Information System authenticator (e.g., password or token) delivered in a secure and confidential way. Passwords shall not be viewable in clear text, except by the account holder.

5. Sharing of passwords

Passwords shall not be transmitted or electronically stored in clear text. No password shall be shared by the user or by the IT and Cybersecurity Department except for temporary passwords provided directly to the user or the user's voice mail by the IT&CS Department. IT&CS passwords are to be kept confidential at all times and not shared with anyone, including agency supervisors.

In cases of lost passwords when the employee is only able to leave a message for the IT&CS staff to reset their password, the IT&CS staff shall do the following:

- a. Reset the password;
- b. Use a randomly selected password as a temporary password for the individual;
- c. Call the employee and provide the temporary password. If the employee is not in, place the information on their voice mail, which is secured and requires their PIN for retrieval.

## 6. Password Setup

Password setup shall be performed in person, or delivered to the user's PIN-protected voicemail. IT&CS will only set temporary passwords that require the user to change the temporary password on first sign-in.

All KRGC terminals shall be configured in a manner that any user ID and password will not be viewable. The computer monitor shall display an asterisk for each key stroke.

KRGC passwords will be stored in the NTLM table, and a fifteen-character password shall be required for all users to ensure Microsoft Windows does not also store it in LM format. The NTLM database will be salted for security. The passwords shall contain the following:

- a. Uppercase
- b. Lowercase
- c. Numerical
- d. Non-alphanumeric character

User passwords shall not contain the user ID, nor be changed more frequently than once per day without system administrator intervention. If a user must change their password more than once a day, they shall contact the staff at IT&CS who will assist with their administrative rights. All passwords shall have a lifespan that does not exceed ninety days and must be different from the previous twenty-four passwords.

System Service Account passwords shall have the following requirements. They shall be constructed with fifteen (15) characters and with the following requirements:

- a. Uppercase

- b. Lowercase
- c. Numerical
- d. Non-alphanumeric character

All System Service Account passwords shall not contain the user ID information, have a lifespan that exceeds ninety (90) days, or match the previous twenty-four (24) passwords.

## 7. Two-Factor-Authentication

KRGC will use both hard token and soft token in obtaining the second One Time Password for the second factor in the authentication.

Hard Tokens shall be issued individually, with a record of the serial number and individual receiving the token. The user shall sign the agreement in Appendix "A" and the agreement shall be kept on file by the IT&CS Department. A log shall be maintained listing the person issuing, the user receiving, and the serial number of the token. The tokens will also be logged to specific equipment.

Soft tokens will be communicated through the agency cell phones assigned to specific staff members. Only agency assigned equipment can be used. The soft token is a backup method, and users allowed soft token use will also have the hard tokens.

In the case of a lost or stolen token, the user is required to report the loss to the IT&CS Department either telephonically or by email at [krgc.support@krgc.ks.gov](mailto:krgc.support@krgc.ks.gov). An incident report will be obtained by the user, and completed for supervisor review within 24 hours of the user's return to the office. These incident cases will be kept on file in the IDPoint system. As soon as possible, the IT&CS Department will issue a new token to the user, deactivate the old token and indicate the token is lost or stolen by flagging it in the soft-token system (currently DUO).

On the day an employee ceases their employment from KRGC, they are required to return their token, computer, cell phone and other IT equipment. Any equipment, including the token, that is not returned will be handled as if it were a security incident. A case number will be obtained, and the Security Director will assign an Agent to investigate.

## 8. Account management

All Information System accounts shall be configured according to the principle of least privilege (PoLP), meaning the user account will only receive those privileges

which are essential to perform its intended function. The needs will be determined by consulting the user's supervisor, not the user.

Separation of duties shall be enforced through account privileges. No individual user account shall have privileges to authorize, perform, review, and audit a single transaction. When available, and applicable, role-based access controls (RBAC) shall be implemented and enforced for systems that contain Restricted-Use Information or systems designated as a Critical System.

## 9. Session management

Information System accounts shall be limited to a maximum of five (5) consecutive failed attempts before being locked. The locked account shall remain locked and require administrator intervention to become unlocked.

### a. Sign-in screen

On sign-in, before the user receives system access, they shall receive a screen with the following information:

Important Notice:

**WARNING!**

You are logging into a system owned and operated by the state of Kansas Racing and Gaming Commission.

This system is allowed for official use only. Unauthorized use is prohibited. This includes access to web pages for personal use or use of email for personal communications.

By using this system, the user consents to interception of information. Users, authorized and unauthorized, have no expectation of privacy. Unauthorized or improper use of this system may result in disciplinary action or criminal or civil penalties.

By clicking "OK" you are accepting the terms of use of this system and consent to the restrictions advised.

Prior to receiving access, the user shall be required to click the [OK] button acknowledging they understand and will comply.

### b. Remote access

KRGC allows for remote access. IT&CS shall authorize Remote Access prior to allowing such connections. Two-Factor-Authentication shall be used for remote access. Any remote access, other than the windows Internet email, shall be by

an agency established encrypted and approved VPN, and traverse managed access points which can be monitored to maintain security.

All remote access shall terminate after a period of thirty (30) minutes of inactivity. Password restrictions will be the same as with any user on the property and require the same notifications and waivers.

The remote access allowed is as follows:

- i. Outlook Web App which accesses the email only and only grants access into the exchange server. The access requires Two-Factor-Authentication with the same method as the Two-Factor-Authentication used with on property equipment.
- ii. Commission pre-meeting access which provides access to current backgrounds. This system is setup the Friday before the meeting, and the password is changed each time. The Commissioners also have tokens to provide the OTP. This also requires Two-Factor-Authentication, the same used on property.
- iii. IT&CS remote access which requires Two-Factor-Authentication, the same used on property and access through a managed access point set up by the IT&CS Department.
- iv. Remote Access for the Disaster Recovery Plan. This will allow access into the warm site from a remote location should the primary site be unavailable due to a man-made or natural disaster. These shall be through KRGC IT&CS Department established VPNs to allow auditing, encryption, and security.

<b>Subject</b>	<b>Number</b> <b>Draft #3</b> <b>2020-10</b>
<b>CYBERSECURITY POLICY SYSTEM CONFIGURATION STANDARD</b>	

<b>Adopted</b> September 11, 2020	<b>Last Revision</b>	<b>Rescinds</b>
--------------------------------------	----------------------	-----------------

<b>Commission Authorization</b>	
---------------------------------	--

Chairman Brandon Jones	Date
------------------------	------

### **I. Purpose/Background**

This policy is promulgated pursuant to the Kansas Cybersecurity Act of 2018, K.S.A. 2018 Supp. 75-7236 through 75-7243, and amendments thereto.

### **II. Introduction**

KRGC makes every effort to ensure the system users have privacy when they use the network. However, there are very infrequent occasions when the use and content of a user file must be accessed to safeguard system security, public and staff safety, or for legal reasons. This policy addresses those needs to safeguard the established, and approved, procedures.

### **III. Overview and Scope**

Kansas Racing and Gaming Information Technology and Cybersecurity is responsible for the protection of the agency's electronic information assets, including performing ongoing and routine network security monitoring, and using technologies to detect and/or prevent network intrusion. Certain laws and regulations also contain security standards that may require the agency to participate in network monitoring, investigation, and the reporting of cyber incidents. This policy describes the technologies in place, the principles for protection of individual privacy, access and retention controls for the data collected or stored, change management processes, and auditing and reporting requirements for the use of network monitoring technologies.

An Advanced Threat Protection (ATP) is used at KRGC in that the IT&CS department focuses on targeting the protection of all data, including sensitive data, with methods that detect, prevent, or eradicate today's sophisticated malware and hacking methods to concentrate on sensitive data. The ATP approach at KRGC is layered, including network devices, the email gateway, malware protection system that provide information to the

Network Consultant, and Director's console to provide alerts and allow them to manage defenses.

#### A. Network Monitoring Technologies

The use of a virus program (currently Sophos) is used to detect known files which are Network monitoring technologies examine network traffic as it passes specific points in the network and may take action to record, alter, or block the traffic in order to protect the sender or the recipient. Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are used to monitor packet activity. As the names indicate, IPS is to prevent a problem from entering the system, and the IDS is used to detect if a threat has entered the system.

Two threat detection techniques are used to detect nefarious packets, signature-based detection and anomaly-based detection. These detection techniques are important when the user is deciding whether to go with a signature or anomaly detection engines.

With the signature-based IDS, or knowledge-based IDS, there are rules or configurations of known malicious traffic being searched for on the packets. Once a match to a signature is found, an alert is sent. To the members of the Information Technology and Cybersecurity unit. These alerts may be for known malware, network scanning activity, and attacks against servers.

With an anomaly-based IDS, or behavior-based IDS, the activity that generated the traffic is far more important than the payload being delivered. An anomaly-based IDS tool does not rely on the signature of the packets. It will search for unusual deviations of activity varying the systems established statistical averages of previous activities (e.g. users who always log into the network from Topeka and accesses licensing files, if the same user logs in from a location off any property and looks at HR files this would generate an alarm to monitor the activity. Then there is the factor of where the IDS focuses its inspections. The first, Network-Based IDS (NIDS) surveils the switches and routers.

Only Information Technology and Cybersecurity is authorized to deploy and operate these technologies on the KRGC network. They will operate these technologies for short-term diagnostic purposes. Any other deployment or operation of network monitoring technologies that will expose traffic other than that of the individual operating the technology shall be approved in advance by Information Technology and Cybersecurity. Depending on the circumstances, review by the Executive Director or his or her designee, and General Counsel, may also be necessary.

In addition to firewalls, antivirus, and email filters, Information Security shall use the following monitoring technologies on the agency network to further the security requirements:

1. KRGC shall run an Intrusion Detection Program to compile the needed logs for Splunk to be fully effective.

2. To provide Intrusion Prevention, KRGC shall use a CISCO firewall with the Next Generation Intrusion Prevention System (NGIPS) feature built into it. This feature shall be activated on the new firewall.
3. KRGC shall use Sophos anti-virus and it shall be updated daily to ensure it has the latest update.
4. Network layer advanced threat protection shall be utilized.
5. KRGC shall establish an IDS system which is both network and host-based.
6. KRGC shall utilize URL/IP-based reputation filtering.
7. KRGC shall secure data with a Data Loss Prevention system.
8. Netflow traffic collector to monitor the network traffic.
9. KRGC shall use Sophos to block unauthorized usage of USB devices. If a staff member desires to use a non-agency issued USB device, they must first obtain permission for the device, and it will only be activated for the minimal time necessary.
10. KRGC shall block access to websites of questionable nature.
11. To provide a zone-GBased Policy Firewall, the Cisco firewalls will be configured with Virtual Fragmentation Reassembly on the zone-based firewall configuration.
12. To provide an adequate Intrusion Detection System, packet monitoring will be conducted with the SNORT program, which is a
13. To provide an adequate Intrusion Prevention System (IPS) the CISCO routers shall be configured to provide the IPS function at all KRGC properties.
14. Any signature-based monitoring system, whether it be an IDS, IPS, or anti-virus, etc. shall be updated immediately when any updates are received by KRGC. Updates will be checked the first of every week.
15. Any other form of monitoring system, whether it be AI based or packet movement monitoring based relying on patches or databases, will be updated as soon as the first Information Technology and Cybersecurity staff member finds there is a new update.

B. Wireless networking

The KRGC network shall be a closed system. Routers with WiFi capability, or any other device allowing WiFi networking, shall never be connected to the KRGC network.

#### C. System changes

1. The following shall be used as needed for system changes
  - a. Change log which contains at least the following:
    - i. date and time of the maintenance;
    - ii. name and organization of the person performing change;
    - iii. name of escort, if required;
    - iv. description of the maintenance performed;
    - v. list of affected Information System(s) Components or component elements;  
and
    - vi. inventory of the system giving the specifications of the Information System Components and the security controls for each component.
  - c. Entities shall maintain an asset inventory of Information Systems' components, update the inventory as changes occur, and review the inventory at least annually.
  - d. The asset inventory shall also identify and document the relationships between each of the Information System Components and the ownership of each component.
  - e. Collaborative infrastructure, such as video and teleconferencing, shall be configured to prohibit remote activation.

#### D. Commitment to Data Privacy

1. Information Security shall take reasonable means to preserve data privacy through the adherence of the following principles. At no time will IT monitor or examine network traffic for any purpose other than protecting the information assets of the agency and in the service of appropriate and legal use and performance of the network.
2. Use of network monitoring technologies to meet the agency's obligations to preserve and provide electronic information in connection with legal proceedings, to investigate allegations of misconduct, and to address threats to the agency or

individuals in a timely manner is governed by the Access to Electronic Information policy 2015-1.

3. Information Technology will not deploy technologies for the purpose of subverting the security of otherwise encrypted communications unless it has obtained the prior approval of the Trustee(s) affected.
4. Information Technology and Cybersecurity will capture and retain network traffic as permitted under the Access to Electronic Information policy and may capture and retain small amounts of network traffic related to specific vulnerabilities to identify security events or confirm a security incident, collect aggregate statistics about network use, and share de-identified or aggregate statistics with peers and information security analysis centers.
5. Information Technology's determination that access to an application or website should be allowed or disallowed will be based upon cybersecurity risk, not the content of the application or website. Blocking for content will be made by the executive director only.

#### E. Retention of Data and Access to Data

As used in this section, a "legitimate business need" means that an employee, based strictly on the employee's job responsibilities, has a specific and articulable reason to access information in order to carry out duties for the agency.

##### 1. Access to and retention of un-redacted data

Network monitoring technologies produce logs that contain real-time, un-redacted, personally identifiable data. The Executive Director shall approve access to these logs in any form for Information Technology and Cybersecurity (IT-CS) staff with a genuine business need for up to 30 days.

##### 2. Access to and retention of redacted data

A redacted data set that does not include raw packet data but may still be personally identifiable, will be exported to the agency's enterprise log management server. The Director of Information Technology shall approve access to the enterprise log management server for the KRGK technology support staff if there is a legitimate business need. Redacted logs shall be retained for up to 365 days.

##### 3. Netflow logs

Netflow logs contain records of network traffic but no content and therefore no personally identifiable information. The Information Technology and Cybersecurity unit may access the Netflow logs if there is a legitimate business need. Netflow logs shall be retained up to 180 days.

4. Extracts and copies of logs

Information Security may retain extracts from redacted or un-redacted logs related to security incidents for longer than 365 days and may share the extracts to resolve security incidents according to business need. Additional copies or exports of the logs are not permitted except as approved by the Director of Information Security.

5. Other access to logs

Use of any network monitoring data for any other purposes, including violation purposes, must be approved by the Executive Director, and the Information Technology Director.

6. Updates to Configuration of Network Monitoring Technologies

Network monitoring technologies require routine maintenance and updates to remain effective. The Director of Information Technology may determine that updated threat intelligence requires manual or automatic implementation of new rules within such technologies.

7. Auditability

KRGC IT and Cybersecurity shall be able to monitor and log all configuration change on the network including individual laptops activity, all manual changes to network monitoring technologies' configuration will be logged.

Due to the large amount of logging activity, there shall be a program which monitors and in itself logs all activity for recall in organized and auditable reports.

8. Reporting

The change log, and any other log, will be provided to the Executive Director, Post Legislative Audit, or Kansas Information Security Office upon request.

9. Data backups

Agency Data shall be backed up daily and backup media stored securely, corresponding with the classification and/or need of the data. RAID-0 shall be used with the system files and RAID-5 on the data files.

F. Firewalls

1. All connections to networks outside the KRGC headquarters, such as the Internet, shall be protected with a firewall that filters both incoming and outgoing network traffic against common threats.

2. All enterprise information systems and any KRGC system hosting confidential data shall be protected by a network firewall and a host-based software firewall, both configured in "default deny" mode for incoming traffic and enforcing documented trust relationships for those systems.
3. All agency computers connected to the KRGC network shall have a host-based firewall configured appropriately for the security requirements of the system and the classification of data stored therein.
4. Logging shall be enabled for all firewalls and periodically reviewed for anomalous events.
5. Configuration of network firewalls and host-based firewalls on enterprise information systems shall be audited periodically to ensure consistency with the security requirements of the system(s) they protect.

#### G. Security event logging and auditing

1. Audit logs recording user activities, exceptions (i.e., errors or failures), and information security events shall be generated commensurate with the security requirements of the system being monitored. Audit logs shall be retained for at least 30 days.
2. Enterprise information systems shall log system administrator activities, such as the use of privileged accounts (e.g., supervisor, administrator, or root).
3. Audit logs shall be reviewed quarterly to detect security violations by the IT and Cybersecurity unit.
4. Security event log data shall be protected against unauthorized access and alteration using Splunk .
5. Clocks of systems being monitored shall be synchronized regularly with the NIST-F1 Cesium Fountain Atomic Clock in Boulder, Colorado. This makes the accuracy to  $3 \times 10^{-16}$  or within in one second in 1000 million years. The accuracy shall be synchronized once a month by IT&CS staff.

#### H. Security management

KRGC's IT security program and policies must be monitored and periodically assessed to ensure their continued effectiveness. The Director of Electronic Security or designee must perform an annual IT security self-assessment and submit a summary report to the Executive Director and the state CISO.

#### I. Security Zones

1. Information on the ID-Point system is all sensitive information. No access will be gained without a unique password being granted by the IT-Cybersecurity unit and the Trustee over the accounts allowed access.
2. Any information extracted from this system shall require the same level of security. For example, background reports will be made available to commissioners monthly, but only after the Trustee authorizes, and IT&CS grants access to, the data with a new password for each time the data will be accessed.
3. During commission meetings a temporary self-standing WI-FI will be established for the commissioners by the Director of IT&CS. The SSID will be concealed when the WI-FI is in service to render it undiscoverable. The WI-FI will have restricted access where only the commissioner's i-Pads will have access. The WI-FI will be taken down by the IT&CS at the conclusion of each commission meeting. This unit will never be connected to the KRGC network. Data is transferred to it by an encrypted drive, requiring password access.

BOOT HILL CASINO & RESORT  
REPORT PRESENTED TO  
THE KANSAS RACING AND GAMING COMMISSION  
September 11, 2020 (Teleconference)

BY: Diane Giardine

- 1) For the month of August 2020, BHCR experienced a decrease in Total Gaming Revenue of 10.32% over prior year August 2019. Total Slot Revenue was down 8.40% and Table Games Revenue was down 24.93%.

Upcoming Promotions & Events

- Weekly Kiosk Games
- Weekly Food and Beverage Specials
- Gift of the Week – Fridays and Sundays
- \$100,000 Big Draw Saturdays

Upcoming Entertainment & Events

- Bridal & Women's Day Out Expo September 13
- 2020 KSHSAA State Volleyball October 30-31
- Jeff Dunham December 11
- Fairy Tales on Ice April 9
- Everclear with Fastball April 24
- Lee Brice May 14

## BOOT HILL CASINO & RESORT

### Lottery Gaming Facility Revenue-Unaudited\*

	August 2020	August 2019	Fiscal YTD 2021	Fiscal YTD 2020
Electronic gaming machines	2,942,883.13	3,213,201.44	5,940,854.14	6,153,533.10
Table games	317,849.36	422,936.56	612,201.78	929,061.61
Other #	<u>99.58</u>	<u>90.39</u>	<u>165.14</u>	<u>136.57</u>
Total Lottery Gaming Facility Revenue	<u>3,260,832.07</u>	<u>3,636,228.39</u>	<u>6,553,221.06</u>	<u>7,082,731.28</u>
State Share 22%	717,383.06	799,970.25	1,441,708.63	1,558,200.88
Local Share 3%	97,824.96	109,086.85	196,596.63	212,481.94
Problem Gambling Share 2%	65,216.64	72,724.57	131,064.42	141,654.63
Casino Share 73%	2,380,407.41	2,654,446.72	4,783,851.37	5,170,393.83

***\*Unaudited-as reported by the Kansas Lottery Central Computer system.***

***#Other sweeps, principally lost and found funds.***

**KANSAS STAR CASINO  
REPORT PRESENTED TO  
THE KANSAS RACING AND GAMING COMMISSION  
September 11, 2020**

**BY:**

**Jeff Babinski – Vice President & General Manager**

**Operational Notes**

- August admissions down 37.4% from August 2019

**August 2020 Gaming Revenue**

- Total Gross Gaming Revenue down 12.1% to August 2019
- Slot Coin-In (Handle) down 9.9% to August 2019
- Slot hold (gross) up 0.6 pts from August 2019
- Table Game drop down 13.4% from August 2019
- Table Game hold is down 2.8 pts from August 2019
- Poker Room revenue down 100% from August 2019 – Remains closed

**Past Arena Events**

- August 22 & 23 - Wichita Flea Market
- August 28 & 29 - Draft Horse Show (Pavilion)

**Upcoming Events**

- September 11 to 13 - Marauders Car Show
- September 26 & 27 - Wichita Flea Market
- October 24 & 25 - Wichita Flea Market

**KANSAS STAR CASINO & RESORT**

**Lottery Gaming Facility Revenue-Unaudited\***

	August 2020	August 2019	Fiscal YTD 2021	Fiscal YTD 2020
Electronic gaming machines	12,553,899.17	13,458,896.82	24,816,880.01	26,894,198.55
Table games	1,581,621.00	2,242,236.64	3,130,429.85	4,410,027.96
Other #	<u>50.17</u>	<u>40.49</u>	<u>99.91</u>	<u>98.12</u>
Total Lottery Gaming Facility Revenue	<u><u>14,135,570.34</u></u>	<u><u>15,701,173.95</u></u>	<u><u>27,947,409.77</u></u>	<u><u>31,304,324.63</u></u>
State Share 22% (Tier 1)**	3,109,825.47	3,454,258.27	6,148,430.15	6,886,951.42
State Share 2% marginal (Tier 2)**	-	-	-	-
Local Share 3%	424,067.11	471,035.22	838,422.29	939,129.74
Problem Gambling Share 2%	282,711.41	314,023.48	558,948.20	626,086.49
Casino Share 73%	10,318,966.35	11,461,856.98	20,401,609.13	22,852,156.98

***\*Unaudited-as reported by the Kansas Lottery Central Computer system.***

***#Other sweeps, principally lost and found funds.***

***\*\* During Kansas Star's Fiscal Year of January 1, 2019 to December 31, 2019, revenue exceeded the tax Tier 1 as stated in their contract. The Tier 2 tax rate was applied to the revenue above Tier 1.***

HOLLYWOOD CASINO AT KANSAS SPEEDWAY  
REPORT PRESENTED TO  
THE KANSAS RACING AND GAMING COMMISSION  
September 11, 2020

BY: RICK SKINNER – VICE PRESIDENT & GENERAL MANAGER

**August 2020**

**Admissions**

- August 2020 admissions were down 41% compared to August of 2019

**August 2020 Revenue Numbers**

- Total Gaming Revenue was \$9.3M – a decrease of 29% compare to last year but an increase of \$800K over last month
- Slot Revenue came in at \$8.8M – a decrease of 24.4%
- Table Games Revenue was \$572K – a decrease of 57%
- The Poker room remains closed

**Recent/Upcoming Events**

- August 28 – Yeti giveaway
- September 4 – Gas Stove giveaway
- September 8 - \$200,000 Pigskin Payoff 2020– dependant upon the duration of the 2020 NFL season.
- September 11 & 18 – Winning Hand promotion
- September 12 – VIP High Limit Pull Party
- September 19 – Raid the Vault giveaway
- September 25 & 26 - \$250,000 Risky Bonus promotion
- October 2 – Red Enamel continuity giveaway
- October 3 – Hollywood Hi-Lo
- October 16 – Hollywood Casino 400 giveaway
- October 18 – *Monster Energy NASCAR Cup Series Hollywood Casino 400*

## HOLLYWOOD CASINO & RESORT

### Lottery Gaming Facility Revenue-Unaudited\*

	August 2020	August 2019	Fiscal YTD 2021	Fiscal YTD 2020
Electronic gaming machines	8,770,585.06	11,606,383.00	16,781,961.07	22,945,014.16
Table games	572,211.78	1,555,647.43	1,072,264.47	2,845,704.17
Other #	<u>58.25</u>	<u>59.18</u>	<u>110.25</u>	<u>104.42</u>
Total Lottery Gaming Facility Revenue	<u>9,342,855.09</u>	<u>13,162,089.61</u>	<u>17,854,335.79</u>	<u>25,790,822.75</u>
State Share 22%	2,055,428.12	2,895,659.71	3,927,953.87	5,673,981.01
Local Share 3%	280,285.65	394,862.69	535,630.07	773,724.68
Problem Gambling Share 2%	186,857.10	263,241.79	357,086.72	515,816.46
Casino Share 73%	6,820,284.22	9,608,325.42	13,033,665.13	18,827,300.61

***\*Unaudited-as reported by the Kansas Lottery Central Computer system.***

***#Other sweeps, principally lost and found funds.***

KANSAS CROSSING CASINO + HOTEL  
REPORT PRESENTED TO  
THE KANSAS RACING AND GAMING COMMISSION  
September 11, 2020  
BY: Jeff McKain

Year over year, Kansas Crossing Casino is reporting the following preliminary results for August;

- - 28.9% Decrease in Admissions
- - 12% Decrease in Coin-In
- - 39% Decrease in Table Drop
- -18.8% Decrease in Net Slot Revenue
- - 19.9% Overall decrease in Net Gaming Revenue

### **Promotions + Events**

- August
  - Casino Hot Seats on Monday the 3<sup>rd</sup> and 17<sup>th</sup>
  - 8X Point Multipliers on Tuesdays.
  - Camp 49 Wednesdays with Hot Seats and lunch specials.
  - Casino Hot Seats on Thursday 13<sup>th</sup> and 27<sup>th</sup>.
  - Casino Hot Seats on Fridays.
  - Bank Account Bonanza Grand Prize drawing on the 31<sup>th</sup>. Possible \$80,000 top prize.
  - Heat Wave promotion on Saturdays.
  - Scratch Card promotion on Sundays.
  - Gift giveaways on the 1<sup>st</sup> (out-door lights), 9<sup>th</sup> (garden carts), 22<sup>nd</sup> (handbags) and 30<sup>th</sup> (Grab Bag).
- September
  - Point Multiplier: Kiosk game every Tuesday.
  - Camp 49 Hot Seats, Fire Floor Hot Seats and lunch specials on Wednesdays.

- Casino Hot Seats every Friday.
- Bank Account Bonanza Grand Prize drawing on Friday the 31st.  
Possible \$90,000 top prize.
- \$500 Frenzie promotion on the 26<sup>th</sup>.
- Casino Gifts every Saturday.
- Hide and Seek \$100K Kiosk game on Sundays.

## KANSAS CROSSING CASINO & RESORT

### Lottery Gaming Facility Revenue-Unaudited\*

	August 2020	August 2019	Fiscal YTD 2021	Fiscal YTD 2020
Electronic gaming machines	2,286,516.54	2,820,314.94	5,061,371.15	5,590,555.37
Table games	146,571.50	217,218.50	280,875.00	474,183.50
Other #	<u>62.15</u>	<u>32.21</u>	<u>119.15</u>	<u>61.43</u>
Total Lottery Gaming Facility Revenue	<u>2,433,150.19</u>	<u>3,037,565.65</u>	<u>5,342,365.30</u>	<u>6,064,800.30</u>
State Share 22%	535,293.04	668,264.44	1,175,320.37	1,334,256.07
Local Share 3%	72,994.51	91,126.97	160,270.96	181,944.01
Problem Gambling Share 2%	48,663.00	60,751.31	106,847.31	121,296.01
Casino Share 73%	1,776,199.64	2,217,422.92	3,899,926.67	4,427,304.22

***\*Unaudited-as reported by the Kansas Lottery Central Computer system.***

***#Other sweeps, principally lost and found funds.***

**August 2020 Casino Financials**

<b>Casino Gaming Revenue for Month Ending August 31, 2020</b>					
Revenue Source	Boot Hill Casino	Kansas Star Casino	Hollywood Casino	Kansas Crossing Casino	Total All Casinos
<b>EGM</b>	\$ 2,942,883	\$ 12,553,899	\$ 8,770,585	\$ 2,286,517	\$ 26,553,884
<b>Table Games</b>	317,849	1,581,621	572,212	146,572	2,618,254
<b>Other #</b>	100	50	58	62	270
<b>Total</b>	\$ 3,260,832	\$ 14,135,570	\$ 9,342,855	\$ 2,433,150	\$ 29,172,408

<b>Cumulative Gaming Revenue per Fiscal Year</b>					
Fiscal Year	Boot Hill	Kansas Star	Hollywood	Kansas Crossing	Total All Casinos
<b>2010</b>	\$ 20,663,987	\$ -	\$ -	\$ -	\$ 20,663,987
<b>2011</b>	40,055,280	-	-	-	40,055,280
<b>2012</b>	43,886,501	98,855,928	54,622,687	-	197,365,116
<b>2013</b>	43,353,504	192,187,166	124,993,721	-	360,534,391
<b>2014</b>	39,906,275	181,079,650	132,036,392	-	353,022,317
<b>2015</b>	40,513,186	181,754,051	142,759,065	-	365,026,302
<b>2016</b>	38,937,088	181,600,677	143,833,330	-	364,371,095
<b>2017</b>	40,222,932	178,105,968	144,582,037	8,206,260	371,117,197
<b>2018</b>	41,186,638	182,084,527	148,770,984	32,465,853	404,508,001
<b>2019</b>	41,589,906	184,157,835	150,790,865	34,489,213	411,027,819
<b>2020</b>	32,971,510	150,355,262	122,114,403	28,620,752	334,061,926
<b>2021</b>	6,553,221	27,947,410	17,854,336	5,342,365	57,697,332
<b>Total Since Opening</b>	\$ 429,840,028	\$ 1,558,128,474	\$ 1,182,357,819	\$ 109,124,443	\$ 3,279,450,764

<b>Fund Distribution FY 2021</b>					
Recipients	Boot Hill	Kansas Star	Hollywood	Kansas Crossing	Total All Casinos
<b>State of Kansas</b>	1,441,709	6,148,430	3,927,954	1,175,320	12,693,413
<b>Local Governments</b>	196,597	838,422	535,630	160,271	1,730,920
<b>Problem Gambling and Addictions Fund</b>	131,064	558,948	357,087	106,847	1,153,947
<b>Casino Manager</b>	4,783,851	20,401,609	13,033,665	3,899,927	42,119,052
<b>Total</b>	6,553,221	27,947,410	17,854,336	5,342,365	57,697,332

<b>Fund Distribution Since Opening</b>					
Recipients	Boot Hill	Kansas Star	Hollywood	Kansas Crossing	Total All Casinos
<b>State of Kansas</b>	94,564,806	342,916,942	260,118,720	24,007,377	721,607,846
<b>Local Governments</b>	12,895,201	46,743,854	35,470,735	3,273,733	98,383,523
<b>Problem Gambling and Addictions Fund</b>	8,596,801	31,162,569	23,647,156	2,182,489	65,589,015
<b>Casino Manager</b>	313,783,220	1,137,305,108	863,121,208	79,660,843	2,393,870,380
<b>Total</b>	429,840,028	1,558,128,474	1,182,357,819	109,124,443	3,279,450,764

*\*Unaudited-as reported by the Kansas Lottery Central Computer system.*

*#Other sweeps, principally lost and found funds.*



## **STAFF AGENDA MEMORANDUM**

**DATE OF MEETING:** September 11, 2020

**AGENDA ITEM:** **FY 2021 & FY 2022 Budgets**

**PRESENTER:** Brandi White, Dir. of Admin, Finance & Audit, Racing and Gaming Comm.  
Stephanie Nickoley, Dir. of Human Resources and Finance State Gaming

**ISSUE SUMMARY:** The annual budget must be submitted to the Division of the Budget on or before September 15, 2020. Prior to submittal, the Commission approves the Racing and Gaming Commission budget, as well as the State Gaming Agency budget. As part of the budget process a revised FY 2020 and requested FY 2021 need to be submitted to the legislature.

### **KRGC General Assumptions**

The budgets for FY 2021 & FY 2022 are based upon the following assumptions: 1) full year of operation for Boot Hill Casino; 2) full year of operation for Kansas Star Casino; 3) full year of operation for Hollywood Casino; 4) full year of operation for Kansas Crossing Casino; 5) no licensed pari-mutuel racing activity; 6) KRGC staff will administer the Kansas Bred Registry Program.

### **FY2020**

KRGC FY 2020 expenditures for racing of \$1,388 were for salaries and wages related to administering the Kansas Horse Registry and regulation of the Kansas Greyhound Registry.

KRGC gaming expenditures for FY 2020 reflect the costs of ongoing regulatory oversight for Boot Hill Casino & Resort, Kansas Star Casino, Hollywood Casino at Kansas Speedway, and Kansas Crossing Casino. Total actual FY 2020 expenditures were approximately \$1 million or 14% below budget at \$6.4 million compared to budgeted expenditures of \$7.5 million. The primary reason for being below budget was related to salaries and wages for unfilled positions.

### **FY 2021**

The KRGC's revised FY 2021 budget is approximately \$7.7 million which is slightly reduced from the approved FY 2021 budget of \$7.8 million. The decrease is attributable to the Governor's allotments specifically the moratorium on death and disability insurance payments. KRGC has

assumed a shrinkage rate of approximately 5% for FY 2020 which totals a shrinkage rate of \$340,000.

The number of FTE positions requested for the FY 2021 budget is unchanged compared to the approved FY 2021 budget, which totals 86.5 FTE. The FTE number does not include a part-time unclassified temporary position under budget policy and procedure guidelines.

Pari-mutuel racing expenses for FY 2021 are expected to be minimal with records storage costs and the administration of the Kansas-Bred Registry Program being the only expenditures.

The budget includes a request to expend from the Illegal Gaming Enforcement fund for operations related to seizure of illegal gambling devices. Funding derived from seizures of illegal gambling devices is authorized by appropriations. The fund is restricted to use for investigatory activities related to illegal gaming.

### **FY 2022**

The KRGC's requested FY 2022 budget is \$7.8 million which is virtually identical to the approved FY 2021 budget of \$7.8 million. KRGC has assumed a shrinkage rate of approximately 5% for FY 2022 which totals a shrinkage amount of approximately \$342,000.

The number of FTE positions requested for the FY 2022 budget is unchanged compared to the approved FY 2021 budget, which totals 86.5 FTE. The FTE number does not include a part-time unclassified temporary position under budget policy and procedure guidelines.

Pari-mutuel racing expenses for FY 2022 are expected to be minimal with records storage costs and the administration of the Kansas-Bred Registry Program being the only expenditures.

The budget includes a request to expend from the Illegal Gaming Enforcement fund for operations related to seizure of illegal gambling devices. Funding derived from seizures of illegal gambling devices is authorized by appropriations. The fund is restricted to use for investigatory activities related to illegal gaming.

Stephanie Nickoley will present the budget for the State Gaming Agency.

**COMMISSION ACTION REQUIRED/REQUESTED:** Commission discussion, consideration and approval of the revised FY 2021 budget and requested FY 2022 budget for the Racing & Gaming Commission.

**STAFF RECOMMENDATIONS:** Staff recommends approval of the proposed budget, subject to technical changes to be made upon entering the budget into IBARS, the State Budget System and to potential future changes made by Division of Budget, the Governor and the Legislature.

Kansas State Gaming Agency  
420 SE 6<sup>th</sup>, Suite 3000  
Topeka, KS 66607



Phone: (785) 368-6202  
Fax: (785) 291-3798  
ksga@ks.gov  
www.ksgaming.org

Kala Loomis, Executive Director

Laura Kelly, Governor

**Meeting:** KRGC September 2020 Meeting  
**Agenda Item:** FY 2021-2022 KSGA Budget  
**Presenter:** Stephanie Nickoley, Director of Human Resources & Finance, State Gaming Agency

### **KSGA Background**

For over 20 years, four tribes have operated casinos pursuant to the tribal-state gaming compacts and the Tribal Gaming Oversight Act. The State Gaming Agency is responsible for ensuring compliance with the Tribal-State Compacts, the Tribal Gaming Oversight Act, and applicable federal and state laws. The four tribes are assessed annually for the Agency's budget.

The Agency's organization is made up of an enforcement unit (made up of sworn law enforcement officers) and a special investigations unit (made up of special investigators – not sworn law enforcement officers), as well as technical and support staff.

The Kansas State Gaming Agency is responsible for conducting background investigations on all employees, gaming vendors, and tribal gaming inspectors connected with the gaming operations at each casino. The Agency also monitors the gaming operation for compliance and has law enforcement authority for criminal activity. Enforcement Agents conduct compliance inspections, monitor gaming activity at tribal casinos and conduct criminal investigations.

### **KSGA Budget Process**

The KSGA is funded based on Section 25 of the compacts with the four Kansas tribes. The compacts state "The state shall annually make an assessment sufficient to compensate the State for the reasonable and necessary costs of regulating Class III gaming pursuant to this Compact. Reimbursable regulatory expenses under this Section shall include all necessary regulatory costs of the State Gaming Agency...." Sec. 25(A).

Section 25(B) states in part, "on or before August 1st, annually, the State shall render to the Tribe a verified, detailed statement of expenses with supporting documentation of the total cost of regulation for the preceding fiscal year ending June 30, together with proposed assessments for the forthcoming fiscal year based on the preceding fiscal year's cost...." In practice, each year just before August 1, KSGA prepares an assessment letter for that fiscal year for each Tribe.

Section 25(B) goes on to say, "On September 1<sup>st</sup> annually, the state, after receiving any objections to the proposed assessments and making such changes or adjustments as may be indicated, shall assess the Tribe for the costs of regulation. The Tribe shall thereafter make a payment representing one-third of the assessment within a 20-day period, and shall make payments thereafter on January 1<sup>st</sup> and April 1<sup>st</sup> annually."

After KSGA goes through the assessment process outlined above with the Tribes, the budget of KSGA must be approved by KRGC according to K.S.A. 74-9803. This statute further explains KRGC role regarding the KSGA. It reads as follows, "The budget of the state gaming agency, the number and qualifications of employees of the state gaming agency and expenditures by the state gaming agency for expenses of dispute resolution pursuant to a tribal-state gaming compact shall be subject to approval by the Kansas racing and gaming commission. All other management functions of the state gaming agency shall be administered by the executive director."

## **Last Year**

In FY2020, the Agency completed 407 individual employee background investigations and 25 vendor background investigations. Each individual tribal gaming commission is responsible for licensing; however, this Agency can, and does when applicable, object to individuals deemed unsuitable for a gaming license. In FY2020 the Agency conducted 157 compliance inspections, handled 2,316 internal control inspections, completed 318 slot machine inspections, and provided or coordinated trainings for 10 outside agency personnel.

## **FY2021**

The KSGA FY2021 budget is approximately \$1.34 million with 13.0 FTE positions. A reduction of 2.5 FTEs from FY2020 was obtained by abolishing unfilled positions within the agency. Revenues are based on the Legislative approved budgets and are paid by the four Tribes. The salaries and wages for the current year will decrease from the FY2020 approved budget to approximately \$1.04 million. The agency will assume a shrinkage amount of \$30,882. The contractual services and commodities budgets will remain consistent from the approved FY2020 budget. KSGA requests a capital outlay budget of \$29,350 to continue replacement of computer equipment, imaging hardware/software and other equipment.

## **FY2022**

The KSGA FY2022 budget is approximately \$1.35 million with 13.0 FTE positions. Revenues are based on the Legislative approved budgets and are paid by the four Tribes. The salaries and wages for the budget year are to provide for a consistent level of employment. Any increases are generally due to the increase in rates for computing fringe benefits. The contractual services and commodities budgets requested are the same as the previous year, \$275,580 and \$24,850 respectively. KSGA requests a capital outlay budget of \$29,350 to continue replacement of computer equipment, imaging hardware/software and other equipment.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME	Kansas Racing and Gaming Commission	
AGENCY NUMBER	553	FUNCTION NO. 1
PROGRAM TITLE AND CODE		
SUBPROGRAM TITLE AND CODE		

**Table of Contents**

General Agency Information - DA 400	.....	2
Explanation of Receipt Estimates - DA 405	.....	8
Racing Program		
Program Narrative Information - DA 400	.....	16
Tribal Gaming Program		
Program Narrative Information - DA 400	.....	23
Expanded Lottery Act Regulation Program		
Program Narrative Information - DA 400	.....	29
Organization Charts	.....	41

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME	Kansas Racing and Gaming Commission	
AGENCY NUMBER	553	Function 1
PROGRAM TITLE AND CODE	Agency-Wide Overview	
SUBPROGRAM TITLE AND CODE		

DIVISION OF THE BUDGET  
STATE OF KANSAS

**KRGC Mission**

The Kansas Racing and Gaming Commission (KRGC) is dedicated to protecting the integrity of racing and gaming in Kansas through enforcement of Kansas laws and regulations, and is committed to preserving and instilling public trust and confidence.

**KRGC Philosophy**

The KRGC approaches its duties with a dedicated sense of purpose and responsibility in service to the public in order to maintain the integrity of gaming, to ensure accountability and compliance with gaming regulations, to educate the public concerning illegal and unregulated gaming operations, to educate operators and the public about responsible gambling practices, and to protect the health, safety and welfare of animals racing at licensed Kansas racetracks.

**Programs Established to Assist with KRGC Mission**

03800 - Expanded Lottery Act Regulation Program  
03900 – Racing Program

**Programs Established to Assist with State Gaming Agency Goals and Objectives (see Tribal Gaming Program narrative for details)**

03700 – Tribal Gaming Program

**KRGC Statutory History**

In 1986, Article 15, Section 3 of the Kansas Constitution was amended by Kansas voters to permit pari-mutuel wagering on horse and greyhound races. The Kansas Pari-mutuel Racing Act was enacted by the Kansas Legislature in 1987 setting forth the terms and conditions of the agency’s operation as enumerated in Chapter 74, Article 88 of the Kansas Statutes Annotated (KSA). The powers and duties of the Kansas Racing Commission, as it was originally named, may be found in K.S.A. 74-8804, as amended. In 1996, the Kansas Racing Commission was renamed the Kansas Racing and Gaming Commission (KRGC) pursuant to K.S.A. 74-8803a.

In 2007, the Kansas Legislature enacted the Kansas Expanded Lottery Act (KELA), which is found in K.S.A. 74-8733 through 74-8773. Under KELA, the Kansas Lottery is authorized to own and operate casino-style games, including slot machines and table games, in specified geographical gaming zones, as well as pari-mutuel racetrack facilities located within certain of those gaming zones. The KRGC, under KELA, regulates and licenses lottery and racetrack gaming facility managers under contract with the Kansas Lottery to operate the games owned by the Kansas Lottery. In addition, the KRGC licenses gaming and non-gaming suppliers used by lottery or racetrack gaming facility managers.

**State Gaming Agency Executive and Statutory History**

In 1995, the State of Kansas by Executive Order No. 95-177 designated the Kansas Department of Commerce & Housing as the State Gaming Agency to carry out certain duties and responsibilities under the gaming compacts entered into with resident Native American Tribes until the Kansas Legislature could enact legislation to designate a permanent State Gaming Agency.

In 1996, the Kansas Legislature enacted the Tribal Gaming Oversight Act, which is set forth in K.S.A. 74-9801 through 74-9809, as amended. Under K.S.A. 74-9803, the State Gaming Agency was attached to the KRGC for budget purposes, human resource assistance, and dispute resolution under the terms of the tribal-state gaming compacts. All other management functions of the State Gaming Agency are administered by its executive director. (See Tribal Gaming Program narrative)

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Agency-Wide Overview
SUBPROGRAM TITLE AND CODE	

DIVISION OF THE BUDGET  
STATE OF KANSAS

**KRGC/Budget Overview**

**Background**

The passage of KELA provided for the creation of four gaming zones in which one lottery gaming facility manager would be selected. In addition, KELA authorized the operation of slot machines at pari-mutuel racetrack facilities under specific conditions. Four lottery gaming facilities have been constructed to date and are in operation in the southwest, northeast, south-central gaming, and southeast gaming zones. Additionally, no licensed pari-mutuel racetrack facilities currently exist in Kansas.

In December 2009 the Boot Hill Casino & Resort (Boot Hill Casino) began operations in Dodge City, Kansas in the southwest gaming zone. Boot Hill Casino has over 600 state-owned slot machines, 16 table games and 5 poker tables. The Boot Hill Casino is flanked on one side by the Dodge City/Ford County United Wireless events and convention center, which includes a 6,000 seat arena, and on the other side by a Hampton Inn that opened in March 2012.

In 2010, Peninsula Gaming, LLC (Peninsula) was selected as the lottery gaming facility manager for the south-central gaming zone. Peninsula constructed a temporary gaming facility known as the Kansas Star Arena Casino that opened in December 2011 in Mulvane, Kansas. The Kansas Star Casino's permanent gaming facility with several dining options opened in December 2012. A connected Hampton Inn with 150 rooms opened in November 2012 and an additional 150 hotel rooms opened in July 2014. The temporary gaming facility has been reconfigured into an entertainment facility. The convention center and the equestrian facilities were completed in January of 2015. Boyd Gaming, Inc. acquired 100% of Peninsula in an equity transaction in November 2012.

The third lottery gaming facility is located in the northeast gaming zone and opened February 2012 in Wyandotte County. The facility, known as the Hollywood Casino at Kansas Speedway (Hollywood Casino), is operated by Kansas Entertainment, LLC, which is a joint venture between Penn National Gaming, Inc. and International Speedway, Corp. International Speedway, Corp. owns and operates the Kansas Speedway and the Hollywood Casino is located on turn two of the Kansas Speedway.

The fourth lottery gaming facility, Kansas Crossing Casino, is located in the southeast gaming zone and opened in March of 2017 in Pittsburg, Kansas. The facility has 625 slot machines, 16 table games, a 123-room Hampton Inn and Suites and a 600 seat entertainment complex.

**KRGC General Assumptions**

The revised FY 2021 and submitted FY 2022 budgets are based upon the following assumptions: 1) full year of operation for Boot Hill Casino; 2) full year of operation for Kansas Star Casino; 3) full year of operation for Hollywood Casino; 4) full year of operation for Kansas Crossing Casino; 5) no licensed pari-mutuel racing activity; 6) KRGC staff will administer the Kansas Bred Registry Program.

The Kansas Bred Registry Program registers Kansas bred horses in various categories for the purpose of distributing moneys credited to the Kansas horse breeding development fund. Distributions from this fund include purse supplements, stakes and awards, and equine research. The registry was previously administered under a contract that expired between the KRGC and the Kansas Horsemen's Association. Although licensed pari-mutuel racing activities are presently dormant, interest in encouraging a resumption of such activities has been high, which warrants the continuation of the registry program. It is also assumed that the KRGC will assume the responsibilities of the Kansas Greyhound Association regarding the administration of the Kansas bred greyhound registry in the future. Under current conditions funding for the maintenance of the registry programs will come from existing State Racing Funds and registration fees deposited into the State Racing Fund.

The KRGC renews its request to continue the practice of using no-limit fee funds for all funds, thus allowing the necessary flexibility to regulate racing and gaming activities as conditions change. Additionally, the KRGC has requested that the current balances in all funds related to pari-mutuel activities be maintained in the event licensed pari-mutuel racing activity resumes in Kansas and to fund the administration of the registry programs.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Agency-Wide Overview
SUBPROGRAM TITLE AND CODE	

DIVISION OF THE BUDGET  
STATE OF KANSAS

**KRGC Budget Overview (continued)**

**Current Year Comparison of FY 2021 Approved and Revised Budget Expenditures**

The KRGC's revised FY 2021 budget is approximately \$7.7 million which is slightly reduced from the approved FY 2021 budget of \$7.8 million. KRGC has assumed a shrinkage rate of 5% for FY 2021 which totals a shrinkage rate of about \$340,000.

The FTE for the requested FY 2021 budget is unchanged from the approved FY 2021 with a total of 86.5 FTE requested. The FTE number does not include a part-time unclassified temporary position under budget policy and procedure guidelines.

Pari-mutuel racing expenses for FY 2021 are expected to be minimal with records storage costs and the administration of the Kansas-Bred Registry Program being the only expenditures.

**Budget Year – Comparison of FY 2021 approved and requested FY 2022 Budget Expenditures**

The KRGC's requested FY 2022 budget is \$7.8 million which is virtually identical to the approved FY 2021 budget of \$7.8 million. KRGC has assumed a shrinkage rate of 5% for FY 2022 which totals a shrinkage amount of approximately \$342,000.

The number of FTE positions requested for the FY 2022 budget is unchanged compared to the approved FY 2021 budget, which totals 86.5 FTE. The FTE number does not include a part-time unclassified temporary position under budget policy and procedure guidelines.

Pari-mutuel racing expenses for FY 2022 are expected to be minimal with records storage costs and the administration of the Kansas-Bred Registry Program being the only expenditures.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME Kansas Racing and Gaming Commission  
AGENCY NUMBER 553  
PROGRAM TITLE AND CODE Agency-Wide Overview  
SUBPROGRAM TITLE AND CODE

DIVISION OF THE BUDGET  
STATE OF KANSAS

**KRGC Budget Overview (continued)**

**KRGC Revenues**

All expenditures by the KRGC are currently paid by the lottery gaming facility managers with the exception of costs associated with the licensing of vendors who pay their own costs. Expenditures are allocated between direct and indirect costs with direct costs being those expenditures identified with a specific lottery gaming facility manager, which primarily includes the cost of the KRGC staff located at each lottery gaming facility. Direct costs account for 65% of total costs. The remaining 35% of total costs are indirect costs that are primarily associated with the Topeka office, and are generally allocated among the lottery gaming facility managers based upon a number of factors (i.e. revenues, direct expenses, number of slot machines and table games, number of employees, etc.). In order for the KRGC to be completely self-funded it bills the lottery gaming facility managers quarterly in advance based upon approved budget expenditures. The first quarterly billings were for six months each to establish the necessary cash balances for ongoing operations. Currently, the KRGC bills for the quarter representing 4-6 months in the future and reconciles quarterly billings to actual expenditures for the quarter just ended making the necessary adjustments to the quarterly billing.

The lottery gaming facility managers also remit payments to cover the cost of the background investigations of their employees. As noted above, certain vendors doing business with lottery gaming facility managers also remit payments to cover the cost of their background investigations. Up front deposits are required based upon an estimate of the total background cost and are supplemented with additional payments if the amount of the deposit is insufficient to cover the actual costs incurred as the background investigation progresses. If the payments received exceed the background costs incurred, the vendor is sent a refund of the unused funds.

**Review of KRGC Prior Year - 2020**

**Racing Program**

KRGC FY 2020 expenditures of \$1,388 were for salaries and wages related to administering the Kansas Horse Registry and regulation of the Kansas Greyhound Registry.

**Expanded Lottery Act Gaming Program**

KRGC expenditures for FY 2020 reflect the costs of ongoing regulatory oversight for Boot Hill Casino & Resort, Kansas Star Casino, Hollywood Casino at Kansas Speedway, and Kansas Crossing Casino. Total actual FY 2020 expenditures were approximately \$1 million or 14% below budget at \$6.4 million compared to budgeted expenditures of \$7.5 million. The primary reason for being below budget was related to salaries and wages for unfilled positions.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME Kansas Racing and Gaming Commission

AGENCY NUMBER 553

DIVISION OF THE BUDGET

PROGRAM TITLE AND CODE Agency-Wide Overview

STATE OF KANSAS

SUBPROGRAM TITLE AND CODE

**Agency Wide Overview of Current Year Estimate and Budget Year Scenarios**

**Current Year - 2021**

**Racing Program**

The budget is built on the assumptions that no pari-mutuel racing is expected to occur in Kansas during FY 2021 and KRGC staff will administer the Kansas Bred Registry Program.

**Tribal Gaming Program**

The Tribal Gaming Program requests no additional funding for FY 2021 and reduced the previously submitted FY2021 budget estimate.

**Expanded Lottery Act Regulation Program**

The current FY 2021 budget is based upon the following assumptions: 1) full year of operation for Boot Hill Casino; 2) full year of operation for Kansas Star Casino; 3) full year of operation for Hollywood Casino; 4) full year of operation for Kansas Crossing Casino.

**Supplemental Package - FY 2021**

**Racing Program**

The Racing Program does not request any supplemental funding for the current year.

**Tribal Gaming Program**

The Tribal Gaming Program does not request any supplemental funding for the current year.

**Expanded Gaming Program**

The Expanded Gaming Program does not request any supplemental funding for the current year.

**Budget Year Information - FY 2022**

**Racing Program**

The budget is built on the assumption that no pari-mutuel racing will occur in Kansas during FY 2022. However, the KRGC will continue the Kansas Bred Registry Program.

**Tribal Gaming Program**

The Tribal Gaming Program current service request is consistent with the current year budget.

**Expanded Lottery Act Regulation Program**

The requested FY 2022 budget is based upon the following assumptions: 1) full year of operation for Boot Hill Casino; 2) full year of operation for Kansas Star Casino; 3) full year of operation for Hollywood Casino; 4) full year of operation for Kansas Crossing Casino.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME Kansas Racing and Gaming Commission

AGENCY NUMBER 553

DIVISION OF THE BUDGET

PROGRAM TITLE AND CODE Agency-Wide Overview

STATE OF KANSAS

SUBPROGRAM TITLE AND CODE

**Agency Wide Overview of Current Year Estimate and Budget Year Scenarios (continued)**

**Supplemental Package - FY 2022**

**Racing Program**

The Racing Program does not request any supplemental packages.

**Tribal Gaming Program**

The Tribal Gaming Program does not request any supplemental packages.

**Expanded Lottery Act Regulation Program**

The Expanded Gaming Program does not request any supplemental packages.

# EXPLANATION OF RECEIPT ESTIMATES

**DA 405**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME:

AGENCY--SUBAGENCY CODES:

PROGRAM TITLE AND CODE:

SUBPROGRAM TITLE AND CODE:

Kansas Racing and Gaming  
Commission

553-00

Racing Program - 03900

## RACING PROGRAM

### State Racing Fund - 5131

K.S.A 74-8826 established the State Racing Fund. All taxes on pari-mutuel wagering, admission tax, application fees and fines must be credited to the fund. The Racing Program is currently on hold as all tracks in the State have ceased operations.

This budget assumes there will be no racing activity to generate revenues or expenditures to this fund in FY 2021, or FY 2022. The operating transfer into the fund in FY 2011 represents the transfer of the outstanding balances in the Horse Fair Racing Benefit Fund, the Racing Investigative Expense Fund, and the Racing Reimbursable Expense Fund to the State Racing Fund at the end of FY 2011. The estimated revenues projected in FY 2020, and FY 2021 are attributed to fees charged for the registration of horses and greyhounds for the Kansas Bred Registry Programs. The registration of horses was formerly administered by the Kansas Horsemen's Association but will now be done by KRGC staff. Additionally, the greyhound registry is currently maintained by the Kansas Greyhound Association and KRGC expects to administer the program in the future.

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Pari-mutuel Tax	-	-	-	-	-	-	-	-	-	-
Pari-mutuel Tax - Simulcast	-	-	-	-	-	-	-	-	-	-
Admissions Tax	-	-	-	-	-	-	-	-	-	-
Charges - Inspect, Examine, Audit	560	1,823	865	409	360	-	-	-	-	-
License Fee - Personal Service	-	-	-	-	-	-	-	-	-	-
License Fee - Business	-	-	-	-	-	758	188	-	1,000	1,000
License Fee - Other	-	-	-	-	-	-	-	-	-	-
Fines	-	-	-	-	-	1,300	-	1,723	-	-
Other Miscellaneous Revenue	-	-	-	-	-	-	-	-	-	-
Operating Transfer In	-	-	-	-	-	-	-	-	-	-
Operating Transfer Out	-	-	-	-	-	-	-	-	-	-
<b>Total Receipts</b>	<b>560</b>	<b>1,823</b>	<b>865</b>	<b>409</b>	<b>360</b>	<b>2,058</b>	<b>188</b>	<b>1,723</b>	<b>1,000</b>	<b>1,000</b>

**EXPLANATION OF RECEIPT ESTIMATES**

**DA 405**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME:  
AGENCY--SUBAGENCY CODES:  
PROGRAM TITLE AND CODE:  
SUBPROGRAM TITLE AND CODE:

Kansas Racing and Gaming  
Commission  
553-00  
Racing Program - 03900

**Horse Fair Racing Benefit Fund - 2296**

K.S.A 74-8838 states that one-third of the simulcast pari-mutuel tax be credited to the County Fair Horse Racing Benefit Fund. Moneys in the horse fair racing benefit fund shall be expended for the following fair meet associated costs: the commission's regulatory costs, tote board expenses, background investigations for fair association or associated non-profit organization's members, purse supplements, operating assistance grants, and the employment of key race officials. The only exception is that the statute allows 25% of moneys credited to the fund, on approval by the Commission, to be used for capital improvements to racetrack facilities.

K.S.A. 74-8747 directs that 1% of net electronic gaming machine income from racetrack facilities be deposited in the Horse Fair Racing Benefit Fund.

**Because this fund is now idle and will not be utilized unless racing resumes, the balance in this fund was transferred to the State Racing Fund to simplify the accounting of idle funds.**

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Simulcast Pari-mutuel Tax	-	-	-	-	-	-	-	-	-	-
Operating Transfer In	-	-	-	-	-	-	-	-	-	-
Balance Transfer Out	-	-	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-	-	-

**Racing Investigative Expense Fund - 2570**

K.S.A. 74-8835 established the Racing Investigative Expense Fund and requires that all receipts other than the application fee received for licensure of facility owners or organizational licensees are to be deposited to the Racing Investigative Expense Fund. Moneys in the fund are to be used for expenses of investigation of an applicant's qualifications for an organization license, facility owner license or facility manager license.

**Because this fund is now idle and will not be utilized unless racing resumes, the balance in this fund was transferred to the State Racing Fund to simplify the accounting of idle funds.**

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Reimbursed Backgrounding Fees	-	-	-	-	-	-	-	-	-	-
Balance Transfer Out	-	-	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-	-	-

**EXPLANATION OF RECEIPT ESTIMATES**

**DA 405**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME:  
AGENCY--SUBAGENCY CODES:  
PROGRAM TITLE AND CODE:  
SUBPROGRAM TITLE AND CODE:

Kansas Racing and Gaming Commission  
553-00  
Racing Program - 03900

**Horse Breeding Development Fund - 2516**

K.S.A. 74-8829 established the Horse Breeding Development Fund. Moneys credited to the Kansas horse breeding development fund must be proportionally categorized by various breeds of horses based upon participation in live races. Money from each category must be used to provide purse supplements, stakes and awards for Kansas-bred horses and research grants to Kansas regents institutions for equine research.

K.S.A. 74-8821 states all horse breakage proceeds be credited to the fund. K.S.A. 74-8767 directs 25% of the net gaming machine income from racetrack facilities deposited to the Live Horse Racing Purse Supplement Fund be transferred to this fund.

This budget assumes there will be no revenue to, or expenditures from, this fund in FY 2020, or FY 2021.

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Breakage	-	-	-	-	-	-	-	-	-	-
Unclaimed Winning Tickets	-	-	-	-	-	-	-	-	-	-
Other Misc Revenue	-	-	-	-	-	-	-	-	-	-
Operating Transfer In	-	-	-	-	-	-	-	-	-	-
Total	-	-	-	-	-	-	-	-	-	-

**Live Horse Racing Purse Supplement Fund - 2546**

K.S.A. 74-8767 establishes the Live Horse Racing Purse Supplement Fund. The statute requires that 25% of moneys deposited to this fund be transferred to the Horse Breeding Development Fund. The remainder of the funds are to be distributed as purse supplements in accordance with rules and regulations adopted by the KRGC with recommendations by the official registering agency. K.S.A. 74-8747 directs 7% of the net gaming machine income from racetrack facilities, up to a maximum of \$3,750 per machine, be deposited to this fund.

This budget assumes there will be no revenue to, or expenditures from, this fund in FY 2021, or FY 2022. There has been no activity in this fund in previous years.

**Live Greyhound Racing Purse Supplement Fund - 2557**

K.S.A. 74-8767 establishes the Live Greyhound Racing Purse Supplement Fund. The statute requires that 25% of the moneys deposited to this fund be transferred to the Greyhound Breeding Development Fund. The remainder of the funds are to be distributed as purse supplements in accordance with rules and regulations adopted by the KRGC with recommendations by the official registering agency. K.S.A. 74-8747 directs 7% of the net gaming machine income from racetrack facilities, up to a maximum of \$3,750 per machine, be deposited to this fund.

This budget assumes there will be no revenue to, or expenditures from, this fund in FY 2021, or FY 2022. There has been no activity in this fund in previous years.

**EXPLANATION OF RECEIPT ESTIMATES**

**DA 405**  
 DIVISION OF THE BUDGET  
 STATE OF KANSAS

AGENCY NAME:  
 AGENCY--SUBAGENCY CODES:  
 PROGRAM TITLE AND CODE:  
 SUBPROGRAM TITLE AND CODE:

Kansas Racing and Gaming  
 Commission  
 553-00  
 Racing Program - 03900

**Racing Reimbursable Expense Fund - 2616**

K.S.A. 74-8827 establishes the Racing Reimbursable Expense Fund and states all fees for processing fingerprints and reimbursements from licensees for the services of assistant animal health officers, stewards and racing judges at racetrack facilities are to be credited to it.

**Because this fund is now idle and will not be utilized unless racing resumes, the balance in this fund was transferred to the State Racing Fund to simplify the accounting of idle funds.**

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Fingerprint Fees	-	-	-	-	-	-	-	-	-	-
Salary Reimbursements	-	-	-	-	-	-	-	-	-	-
Balance Transfer Out	-	-	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-	-	-

**Racing Applicant Deposit Fund - 7383**

K.S.A. 74-8828 establishes the Racing Applicant Deposit Fund. K.S.A. 74-8815 directs the application deposit fee for a facility owner's license shall be credited to the Racing Applicant Deposit Fund with interest accruing monthly.

There are currently no deposits to this fund and these estimates are based on the assumption there will not be a licensed operational track in FY 2021, or FY 2022.

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Interest	-	-	-	-	-	-	-	-	-	-

**EXPLANATION OF RECEIPT ESTIMATES**

**DA 405**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME:  
AGENCY--SUBAGENCY CODES:  
PROGRAM TITLE AND CODE:  
SUBPROGRAM TITLE AND CODE:

Kansas Racing and Gaming Commission  
553-00  
Racing Program - 03900

**Greyhound Breeding Development Fund - 2601**

K.S.A. 74-8831 established the Greyhound Breeding Development Fund and requires that all moneys credited to this fund be used only for the benefit of greyhounds. The statute directs moneys to be used as follows: 15% is credited to the greyhound tourism fund, 35% for research conducted within the state of Kansas relating to the prevention of injury to and disease of greyhounds; 50% for purse supplements, and an amount determined by the commission, but not to exceed \$30,000 is used to pay a portion of the administrative costs of the official registering agency.

K.S.A. 74-8822 states all monies from unclaimed winning ticket wagers on greyhounds be credited to this fund. K.S.A. 74-8767 directs 25% of the net gaming machine income from racetrack facilities deposited to the Live Greyhound Racing Purse Supplement Fund be transferred to this fund.

The remainder of the moneys in this fund at the end of FY 2013 were swept by the legislature at the beginning of FY 2014. This budget assumes that there will be no revenue to, or expenditures from this fund in FY 2021, or FY 2022.

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Other	-	-	-	-	-	-	-	-	-	-
Unclaimed Winning Tickets	-	-	-	-	-	-	-	-	-	-
Operating Transfers Out	-	-	-	-	-	-	-	-	-	-
Transfer Out (Swept by Legislature)	-	(87,012)	-	-	-	-	-	-	-	-
	-	(87,012)	-	-	-	-	-	-	-	-

**Greyhound Promotion and Development Fund - 2561**

K.S.A. 74-8842 creates the Greyhound Promotion and Development Fund and is funded through a voluntary greyhound purse check off program which provides for the deduction of 2% from all purses paid to kennels and greyhound owners who participate in the program. Greyhound owners and kennel operators are provided the opportunity annually not to participate in the program. Moneys deposited into the fund are distributed to the official greyhound registering agency and are to be used only for the development, promotion and representation of the greyhound industry in Kansas.

Language was included in the appropriations bill for the 2009 and 2010 legislative sessions that redirected the 15% transfer from the Greyhound Breeding Development Fund to the Greyhound Tourism Fund (in the Department of Commerce) to this fund.

The remainder of the moneys in this fund at the end of FY 2013 were swept by the legislature at the beginning of FY 2014. This budget assumes that there will be no revenue to, or expenditures from this fund in FY 2021, or FY 2022.

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Operating Transfer In	-	-	-	-	-	-	-	-	-	-
Other Misc Revenue	-	-	-	-	-	-	-	-	-	-
Transfer Out (Swept by Legislature)	-	(39,681)	-	-	-	-	-	-	-	-
	-	(39,681)	-	-	-	-	-	-	-	-

**EXPLANATION OF RECEIPT ESTIMATES**

AGENCY NAME: Kansas Racing and Gaming Commission

DA 405  
 DIVISION OF THE BUDGET  
 STATE OF KANSAS

AGENCY--SUBAGENCY CODES: 553-00  
 PROGRAM TITLE AND CODE: Tribal Gaming Program - 03700  
 SUBPROGRAM TITLE AND CODE: DOB USE ONLY

FUNCTION NO. 01

**TRIBAL GAMING PROGRAM**

Tribal Gaming Fund - 2320

Revenues are based on the Legislative approved budgets and are approved and paid by the compacted tribes.

	<u>FY19</u>	<u>FY20</u>	<u>FY21</u>	<u>FY21</u>
Other Service Charges	1,611,736	1,543,231	1,343,690	1,353,809
Interchange of Gvt Employee Payroll				
Operating Transfer In	450,000	450,000	450,000	450,000
Operating Transfer Out	(450,000)	(450,000)	(450,000)	(450,000)

**EXPLANATION OF RECEIPT ESTIMATES**

**DA 405**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME:

AGENCY--SUBAGENCY CODES:

PROGRAM TITLE AND CODE:

SUBPROGRAM TITLE AND CODE:

Kansas Racing and Gaming Commission

553

Expanded Gaming Program - 03800

**EXPANDED GAMING PROGRAM**

**Expanded Lottery Act Regulation Fund - 2535**

The Kansas Expanded Lottery Act specifies that the cost of regulation is to be incurred by the lottery gaming facility managers. In 2007, the KRGC obtained a loan from the PMIB to finance expanded gaming regulation until the lottery gaming facility managers were selected and approved. During the 2008 legislative session, the amount of the loan from PMIB was increased to \$5,000,000 to cover KRGC operating costs for FY 2009 and FY 2010 and the term of the loan was extended through FY 2012. The balance of the loan was repaid in FY 2012.

Revenue projections for FY 2021 and FY 2022 include billings and payments from the currently operating casinos for the KRGC's direct and indirect costs associated with the operations of the Hollywood Casino, the Kansas Star Casino, the Boot Hill Casino, and the Kansas Crossing Casino. Payments are received in advance of expenditure on a quarterly billing cycle.

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
PMIB Loan Proceeds	-	-	-	-	-	-	-	-	-	-
LGFRB applicant reimbursements	-	-	940,717	-	-	-	-	-	-	-
Hollywood Start-up Reimb.	-	-	-	-	-	-	-	-	-	-
Sumner Casino Start-up Reimb.	-	-	-	-	-	-	-	-	-	-
Boot Hill Start-up Reimb.	-	-	-	-	-	-	-	-	-	-
Hollywood Ops Reimbursement	1,805,619	1,763,838	1,933,256	1,967,293	1,753,827	1,807,405	1,754,182	1,368,001	2,147,829	2,073,698
Sumner Casino Ops Reimbursement	1,839,796	1,754,662	1,795,434	1,923,542	1,825,345	1,865,898	1,907,527	1,474,782	2,048,265	2,246,512
Boot Hill Ops Reimbursement	1,116,453	977,529	967,534	1,102,789	942,606	982,583	1,090,169	732,669	1,330,903	1,377,197
KS Crossing OPS Reimbursement	-	-	-	-	1,879,359	1,088,448	1,162,074	883,327	1,721,384	1,378,170
Facility Mgr Background Deposits	-	-	-	-	-	-	-	-	-	-
Vendor Background Fees	-	-	-	-	-	-	-	-	-	-
Miscellaneous Revenue	1,442	-	98,671	(1,205)	3,675	388	4,695	35,806	-	-
ELARF Transfer	-	-	-	-	-	-	-	-	-	-
Transfer Out	-	-	-	-	-	-	-	-	-	-
	<u>4,763,310</u>	<u>4,496,029</u>	<u>5,735,612</u>	<u>4,992,419</u>	<u>6,404,812</u>	<u>5,744,722</u>	<u>5,918,647</u>	<u>4,494,585</u>	<u>7,248,381</u>	<u>7,075,577</u>

**EXPLANATION OF RECEIPT ESTIMATES**

**DA 405**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME: Kansas Racing and Gaming Commission  
 AGENCY--SUBAGENCY CODES: 553  
 PROGRAM TITLE AND CODE: Expanded Gaming Program - 03800  
 SUBPROGRAM TITLE AND CODE:

**Gaming Background Investigations Fund - 2682**

The Gaming Background Investigations Fund is established by appropriations act to be used for deposits by gaming and non-gaming vendors for background investigation costs. Expenses for backgrounds will be charged to this fund and tracked individually by project code for each vendor as each vendor is entitled to a refund of unspent deposits.

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Examination Deposits	378,633	194,128	299,445	199,340	176,153	138,652	175,742	130,155	250,000	275,000
Refunds	(44,056)	(38,858)	-	-	(9,440)	-	-	-	-	-
	<u>334,577</u>	<u>155,270</u>	<u>299,445</u>	<u>199,340</u>	<u>166,713</u>	<u>138,652</u>	<u>175,742</u>	<u>130,155</u>	<u>250,000</u>	<u>275,000</u>

**Education and Training Fund - 2459**

The KRGC Education and Training Fee Fund is established by appropriations act and its purpose is to allow the KRGC to receive and expend funds for training opportunities that could be offered to others outside of the KRGC. This fund is not budgeted and is used only as training opportunities arise. In FY 2021 and FY 2022, time permitting, we plan to seek out training opportunities for in-house staff and to invite employees from other agencies to help offset our training costs.

**Illegal Gaming Enforcement Fund - 2734**

The KRGC became the primary coordinator for state-level illegal gambling complaints after the passage of the Expanded Lottery Act, but no funds were appropriated for its activities. The Illegal Gaming Enforcement Fund was established during the 2011 legislative session and initial funding of \$5,000 was provided via a transfer from the state racing fund. A proviso was included that would allow KRGC the ability to retain funds seized as part of illegal gaming enforcement operations. For this budget submission we would again request that the proviso included for the FY 2015 appropriations act be retained for the FY 2021, and FY 2022 appropriations.

- (1) A proviso that would allow KRGC the ability to retain funds seized as part of illegal gaming enforcement operations and deposited into the fund to be used for illegal gaming enforcement activities.
- (2) A proviso that would allow the KRGC to receive moneys from state or federal seizures or awards related to illegal gaming enforcement activities of the agency.
- (3) The fund is a no-limit fund so that monies may be used in a timely manner for enforcement activities.

	Actual FY13	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Seizures	-	5,996	13,664	2,925	-	60	(919)	113,908	5,000	5,000
Transfers	-	-	-	-	-	-	-	-	-	-
	<u>-</u>	<u>5,996</u>	<u>13,664</u>	<u>2,925</u>	<u>-</u>	<u>60</u>	<u>(919)</u>	<u>113,908</u>	<u>5,000</u>	<u>5,000</u>

**Gaming Machine Examination Fund - 2998**

KRGC requests that the Gaming Machine Examination Fund be re-established as a no-limit fee fund for the purpose of receiving certification fees from electronic gaming machine manufacturers to meet the requirements of K.S.A. 74-8750(c). All revenues received for the Gaming Machine Examination Fund will be from electronic gaming equipment manufacturers and any unused funds will be returned to the appropriate vendor.

	Actual FY14	Actual FY15	Actual FY16	Actual FY17	Actual FY18	Actual FY19	Actual FY20	Estimate FY21	Estimate FY22
Gaming Machine Exam Deposits	-	-	-	-	-	-	-	-	-
	<u>-</u>	<u>-</u>							

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Parimutuel Gaming Program - 03900
SUBPROGRAM TITLE AND CODE	Racing Regulation

**PARIMUTUEL GAMING PROGRAM**  
*Subprogram Racing Regulation*

**Purpose:**

The commission's primary purpose is to regulate the pari-mutuel industry through enforcement of the Kansas parimutuel racing act, K.S.A. 74-8801, et seq., and rules and regulations adopted by the commission. The commission also collects pari-mutuel taxes and promotes the pari-mutuel industry through the Kansas-bred development funds for horses and greyhounds and the horse fair racing benefit fund.

**Required By Statute:** Yes.

**Maintenance of Effort or Matching Requirement:** None.

**Statutory Requirements:** K.S.A. 74-8801 through 74-8842.

**Consequences of Not Funding:** Currently, there are breeders of horses and greyhounds who continue to register their animals as Kansas bred. Not funding this program would result in their being no mechanism for these breeders to be able to register their animals as Kansas bred. The distinction can be important within the industry and not having this mechanism may have a negative impact on some breeders. Not funding this program would result in the loss of historical documents prior to their approved destruction.

**PROGRAM'S STATUTORY HISTORY:**

**K.S.A. 74-8804 (a)** through (q) require the commission to observe and inspect all racetrack facilities; administer oaths and take depositions; examine any books, paper records or memoranda of any licensee, racetrack or business involved in simulcasting races to racetrack facilities in Kansas; issue subpoenas; allocate race meeting dates, racing days, and hours to all organization licensees; authority to exclude, or cause to be expelled from any race meeting or racetrack facility or to prohibit a licensee from conducting business with any person who has violated the provision of this act or any rule and regulation or order of the commission, been convicted of a violation of the racing or gambling laws or has been adjudicated of committing as a juvenile an act which if committed by an adult, would constitute such a violation, whose person reflects adversely on the honesty and integrity of horse or greyhound racing or interferes with the conduct of a race meeting; review and approve all proposed construction and major renovations to racetrack facilities; review and approve all proposed contracts with racetracks or businesses involved in simulcasting races to racetrack facilities in Kansas; suspend a horse or greyhound from participation in races; impose a civil fine; adopt rules and regulations and require fingerprinting and background information of all persons for employment, license or simulcasting license.

**PROGRAM GOAL**

To maintain the integrity of pari-mutuel wagering systems and to protect the public and the health, safety and welfare of the racing animal.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Parimutuel Gaming Program - 03900
SUBPROGRAM TITLE AND CODE	

DIVISION OF THE BUDGET  
STATE OF KANSAS

**PARIMUTUEL GAMING PROGRAM**

**Salaries and Wages**

	<b>FY13</b>	<b>FY14</b>	<b>FY15</b>	<b>FY16</b>	<b>FY17</b>	<b>FY18</b>	<b>FY19</b>	<b>FY20</b>	<b>FY21</b>	<b>FY22</b>
	<b>Actual</b>	<b>Estimate</b>	<b>Estimate</b>							
State Racing Fund	1,290	7,743	2,127	4,864	4,895	1,406	342	1,388	3,026	3,060
Horse Fair Racing Benefit Fund	-	-	-	-	-	-	-	-	-	-
Racing Investigative Expense Fund	-	-	-	-	-	-	-	-	-	-
Racing Reimbursable Expense Fund	-	-	-	-	-	-	-	-	-	-
<b>Total</b>	<b>1,290</b>	<b>7,743</b>	<b>2,127</b>	<b>4,864</b>	<b>4,895</b>	<b>1,406</b>	<b>342</b>	<b>1,388</b>	<b>3,026</b>	<b>3,060</b>

**Prior Year FY 2020**

In FY20 \$1,388 in salaries and wages were expended to maintain the Kansas Bred Registry. The Kansas Bred Registry was previously maintained by contract by the Kansas Horseman's Association.

**Current Year FY 2021**

A small part (.10) of one FTE regular classified position is budgeted to maintain the Kansas Bred Registry Program. Some horse owners have elected to continue to register their horses in the event that pari-mutuel racing resumes. In FY 2020 the Kansas Greyhound Association continued to register Kansas bred greyhounds. However, it is anticipated that KRGK will take over the registration of Kansas bred greyhounds in the future.

**Budget Year FY 2022**

A small part (.10) of one FTE regular classified position is budgeted to maintain the Kansas Bred Registry Program. Some horse owners have elected to continue to register their horses in the event that pari-mutuel racing resumes. In FY 2020 the Kansas Greyhound Association continued to register Kansas bred greyhounds. However, it is anticipated that KRGK will take over the registration of Kansas bred greyhounds in the future.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Parimutuel Gaming Program - 03900
SUBPROGRAM TITLE AND CODE	

**PARIMUTUEL GAMING PROGRAM**

**Contractual Service**

**State Racing Fund**

	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21	FY22
	Actual	Estimate	Estimate							
Communication	-	-	-	-	-	-	-	-	-	-
Freight & Express	-	-	-	-	-	-	-	-	-	-
Printing & Advertising	-	-	-	-	-	-	-	-	-	-
Rents	470	-	422	1,045	308	-	268	-	500	500
Repairing & Servicing	-	284	-	-	-	-	-	-	-	-
Travel & Subsistence	(154)	-	-	-	-	-	-	-	-	-
Fees - Other Services	-	-	-	-	-	-	-	-	-	-
Fees - Professional Services	-	-	-	-	-	-	-	-	500	500
Other Contractual Services	-	-	-	-	-	-	-	-	-	-
Total Contractual Services	316	284	422	1,045	308	-	268	-	1,000	1,000

**Prior Year FY 2020**

No funds were expended.

**Current Year FY 2021**

Funds are budgeted for racing records storage and to operate the Kansas Bred Registry Program for registration of horses. Some horse owners have elected to continue to register their horses in the event that pari-mutuel racing resumes. Additionally, KRGK anticipates that the agency will maintain registry for Kansas bred greyhounds in the future.

**Budget Year FY 2022**

Funds are budgeted for racing records storage and to operate the Kansas Bred Registry Program for registration of horses and greyhounds. Some horse owners have elected to continue registration in the event that pari-mutuel racing resumes. Additionally, KRGK anticipates that the agency will maintain registry for Kansas bred greyhounds in the future.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553  
 PROGRAM TITLE AND CODE Parimutuel Gaming Program - 03900  
 SUBPROGRAM TITLE AND CODE

DIVISION OF THE BUDGET  
 STATE OF KANSAS

**PARIMUTUEL GAMING PROGRAM**

**Contractual Services (continued)**

**Other Funds**

	<b>FY13</b>	<b>FY14</b>	<b>FY15</b>	<b>FY16</b>	<b>FY17</b>	<b>FY18</b>	<b>FY19</b>	<b>FY20</b>	<b>FY21</b>	<b>FY22</b>
	<b>Actual</b>	<b>Estimate</b>	<b>Estimate</b>							
Horse Fair Racing Benefit Fund	-	-	-	-	-	-	-	-	-	-
Kansas Horse Breeding Development Fund	-	-	-	-	-	-	-	-	-	-
Racing Investigative Expense Fund	-	-	-	-	-	-	-	-	-	-
Kansas Greyhound Breeding Development Fund	-	-	-	-	-	-	-	-	-	-
Racing Reimbursable Expense Fund	-	-	-	-	-	-	-	-	-	-
Total Contractual Services	-	-	-	-	-	-	-	-	-	-

**Prior Year FY 2020**

No funds were expended.

**Current Year FY 2021**

No funds are budgeted.

**Budget Year FY 2022**

No funds are budgeted.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553  
 PROGRAM TITLE AND CODE Parimutuel Gaming Program - 03900  
 SUBPROGRAM TITLE AND CODE

DIVISION OF THE BUDGET  
 STATE OF KANSAS

**PARIMUTUEL GAMING PROGRAM**

Commodities

**State Racing Fund**

	<b>FY13</b>	<b>FY14</b>	<b>FY15</b>	<b>FY16</b>	<b>FY17</b>	<b>FY18</b>	<b>FY19</b>	<b>FY20</b>	<b>FY21</b>	<b>FY22</b>
	<b>Actual</b>	<b>Estimate</b>	<b>Estimate</b>							
Animal Food	-	-	-	-	-	-	-	-	-	-
Maintenance Material, Supplies, Parts	-	-	-	-	-	-	-	-	-	-
Motor Vehicle Parts, Supplies	38	-	-	-	-	-	-	-	-	-
Professional & Scientific Supplies	-	-	-	-	-	-	-	-	-	-
Stationary & Office Supplies	26	-	-	-	-	-	-	-	-	-
Other Supplies, Materials, Parts	-	-	-	-	-	-	-	-	-	-
<b>Total Commodities</b>	<b>64</b>	<b>-</b>	<b>-</b>							

Prior Year FY 2020

No funds were expended.

Current Year FY 2021

No funds are budgeted.

Budget Year FY 2022

No funds are budgeted.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME  
AGENCY NUMBER  
PROGRAM TITLE AND CODE  
SUBPROGRAM TITLE AND CODE

Kansas Racing and Gaming Commission  
553  
Parimutuel Gaming Program - 0390

**PARIMUTUEL GAMING PROGRAM**

**Capital Outlay**

**State Racing Fund**

	<b>FY13</b>	<b>FY14</b>	<b>FY15</b>	<b>FY16</b>	<b>FY17</b>	<b>FY18</b>	<b>FY19</b>	<b>FY20</b>	<b>FY21</b>	<b>FY22</b>
	<b>Actual</b>	<b>Estimate</b>	<b>Estimate</b>							
Equipment, Machinery, Furniture and Fixtures	-	-	-	-	-	-	-	-	-	-
Books and Library Materials	-	-	-	-	-	-	-	-	-	-
Professional and Scientific Equipment	-	-	-	-	-	-	-	-	-	-
Microcomputer Systems and Support Equipment	-	-	-	-	-	-	-	-	-	-
Information Processing Equipment	-	-	-	-	-	-	-	-	-	-
Computer Systems, Info Processing or Micro Software	-	-	-	-	-	-	-	-	-	-
Other Equip Furniture/Fixtures	-	-	-	-	-	-	-	-	-	-
Passenger cars	-	-	-	-	-	-	-	-	-	-
Total Capital Outlay	-	-	-	-	-	-	-	-	-	-

**Prior Year FY 2020**

No funds were expended

**Current Year FY 2021**

No funds are budgeted.

**Budget Year FY 2022**

No funds are budgeted.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553  
 PROGRAM TITLE AND CODE Parimutuel Gaming Program - 03900  
 SUBPROGRAM TITLE AND CODE

**PARIMUTUEL GAMING PROGRAM**

**Other Assistance, Grants, Benefits**

**All Funds**

	<b>FY13</b>	<b>FY14</b>	<b>FY15</b>	<b>FY16</b>	<b>FY17</b>	<b>FY18</b>	<b>FY19</b>	<b>FY20</b>	<b>FY21</b>	<b>FY22</b>
	<b>Actual</b>	<b>Estimate</b>	<b>Estimate</b>							
State Racing fund	-	-	-	-	-	-	-	-	-	-
Horse Fair Horse Racing Benefit Fund	-	-	-	-	-	-	-	-	-	-
Kansas Horse Breeding Development Fund	-	-	-	-	-	-	-	-	-	-
Kansas Greyhound Breeding Development Fund	-	-	-	-	-	-	-	-	-	-
Live Greyhound Purse Supplement Fund	-	-	-	-	-	-	-	-	-	-
Greyhound Promotion and Development Fund	-	-	-	-	-	-	-	-	-	-
Live Horse Racing Purse Supplement Fund	-	-	-	-	-	-	-	-	-	-
<b>Total Other Assistance, Grants, Benefits</b>	<b>-</b>	<b>-</b>								

**Prior Year FY 2020**

No funds were expended.

**Current Year FY 2021**

No funds are budgeted.

**Budget Year FY 2022**

No funds are budgeted.

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553      FUNCTION NO.      1
PROGRAM TITLE AND CODE	Tribal Gaming Program - 03700
SUBPROGRAM TITLE AND CODE	

**TRIBAL GAMING PROGRAM**

The Tribal Gaming Program fulfills the duties and obligations of the state as set forth in the tribal-state gaming compacts and the Tribal Gaming Oversight Act. There are four Native American tribes in Kansas which have approved tribal-state gaming compacts which have been approved by the Kansas legislature, signed by the Governor and approved by the Bureau of Indian Affairs. These four nations are: the Iowa's Tribe of Kansas and Nebraska; the Kickapoo Tribe of Kansas; the Prairie Band Potawatomi Nation; and the Sac & Fox Nation of Missouri in Kansas and Nebraska.

**PROGRAM'S STATUTORY HISTORY:**

K.S.A. 74-9801 through 74-9809 (a) mandate the agency shall be responsible for oversight, monitoring and compliance of class III gaming conducted pursuant to tribal-state compacts. It is the responsibility of the agency to monitor compliance with tribal-state gaming compacts and perform the duties of the state gaming agency as provided for in the tribal-state gaming compacts. The agency may examine and inspect all tribal gaming facilities and facilities linked to Kansas tribal gaming facilities for gaming, including but not limited to all machines and equipment used for tribal gaming, books, papers, records, electronic records, computer records or surveillance and security tapes and logs of any tribal gaming facility. The executive director may issue subpoenas. The agency can review all licensing and disciplinary actions and reports of noncompliance with the tribal-state compacts. Enforcement agents are vested with the power and authority of law enforcement officers.

**PROGRAM GOAL**

Ensure compliance with the four tribal-state compacts and the Tribal Gaming Oversight Act and that gaming is conducted in accordance with said compacts and applicable state and federal laws; protect the state of Kansas and its citizens from criminal activity in the Tribal gaming arena; ensure accurate and complete information is provided to the different tribal gaming commissions for licensing purposes and to review all licensing decisions to ensure compliance; to conduct thorough background investigations on all gaming employees, management contractors, manufacturers and distributors of gaming devices seeking licensure at gaming facilities located in this state; investigate any alleged violations of the tribal-state compacts and the Tribal Gaming Oversight Act.

**OBJECTIVES:**

Prohibit undesirable elements from obtaining licenses and access to casino facilities and activities.

Ensure the provisions of the tribal-state gaming compacts, the Tribal Gaming Oversight Act and the Indian Gaming Regulatory Act are met.

	AGENCY NAME	Kansas Racing and Gaming Commission
	AGENCY NUMBER	553                      FUNCTION NO.    1
	PROGRAM TITLE AND CODE	Tribal Gaming Program - 03700
	SUBPROGRAM TITLE AND CODE	

**TRIBAL GAMING PROGRAM**

**OUTCOME MEASURES:**

	FY19	FY20	FY21	FY22
	Actual	Actual	Estimate	Estimate
Average days to complete background investigations	41	40	45	45
Average days to preliminary suitability	1	2	2	2

**STRATEGIES:**

- Conduct all category I and category II background investigations with employees of the Tribal Gaming Program.
- Conduct investigations and inspections of the gaming operations.
- Conduct training of tribal gaming personnel on gaming operations.

**OUTPUT MEASURES:**

	FY19	FY20	FY21	FY22
	Actual	Actual	Estimate	Estimate
Number of background investigations.	514	432	470	470
Number of official slot machine inspections	342	318	400	400
Number of compliance inspections	230	457	200	200
Number of internal control inspections (NEW during FY16)	3,271	2,316	2,750	2,750
Number of outside agency personnel trained	38	10	25	25

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME  
AGENCY NUMBER  
PROGRAM TITLE AND CODE  
SUBPROGRAM TITLE AND CODE

Kansas Racing and Gaming Commission  
553  
Tribal Gaming Program - 03700

FUNCTION NO. 1

**TRIBAL GAMING PROGRAM**

Salaries and Wages

Tribal Gaming Fund	FY 19 Actual	FY 20 Actual	FY 21 Estimate	FY 22 Estimate
	1,128,150	1,130,427	1,044,792	1,054,911
Assumed Shrinkage			30,882	30,882
Net Salaries and Wages			1,013,910	1,024,029

The Tribal Gaming Program funding request will be used to finance 13 FTE positions for FY 21 & FY 22.

This is a decrease of 2.5 FTE positions from FY 2020. The decrease was obtained by abolishing vacant positions.

The Tribal Gaming Program will be performing all the background investigations necessary for category I and category II employees, manufacturers and distributors.

Current Year

Salaries and wages for the current year decreased from the FY 20 legislative approved budgeted amount.

The Kansas State Gaming Agency has assumed a shrinkage amount of \$30,882, which equals a shrinkage rate of approximately 2.96%.

Budget Year FY 2021

Salaries and wages for the budget years are to provide for a consistent level of employment.

The Kansas State Gaming Agency will assume a shrinkage amount of \$30,882, which equals a shrinkage rate of approximately 2.93%.

Enhancement

There are no salary and wage enhancements for the Tribal Gaming Program in the budget year.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553 FUNCTION NO. 1  
 PROGRAM TITLE AND CODE Tribal Gaming Program - 03700  
 SUBPROGRAM TITLE AND CODE

**TRIBAL GAMING PROGRAM**

Contractual Services

Tribal Gaming Fund	FY19	FY20	FY21	FY22
	Actual	Actual	Estimate	Estimate
Communication	36,472	35,186	40,765	40,765
Freight & Express	7	16	-	-
Printing & Advertising	24	28	200	200
Rents	89,654	91,673	89,200	89,200
Repairing & Servicing	15,149	15,706	24,800	24,800
Travel & Subsistence	7,067	2,924	25,415	25,415
Fees - Record Checks, Building Surcharge	22,055	38,203	51,500	51,500
Fees - Other Services	27,541	39,805	36,000	36,000
Fees - Professional Services	15	15	1,000	1,000
Other Contractual Services	2,809	2,536	5,700	5,700
Official Hospitality	50	52	1,000	1,000
<b>Total Contractual Services</b>	<b>200,843</b>	<b>226,144</b>	<b>275,580</b>	<b>275,580</b>

Prior Year FY 2020

During FY 20, Contractual Services were approximately 17.94% below the legislative approved budget. The tribes are given a credit for the amounts below the budget to the current year's assessments.

Current Year FY 2021

In the current year, the contractual service budget remains consistent with the FY 20 legislative approved budgeted amount.

Budget Year FY 2022

In the budget year FY21, the contractual services budget remains consistent with the current year budget.

NOTE: The Tribal Gaming Program requests to continue the Hospitality Fund in the amount of \$1,000 for purpose of hosting meetings.

Enhancement

There are no contractual service enhancements for the Tribal Gaming Program in the budget year.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME  
AGENCY NUMBER  
PROGRAM TITLE AND CODE  
SUBPROGRAM TITLE AND CODE

Kansas Racing and Gaming Commission  
553      FUNCTION NO.  
Tribal Gaming Program - 03700

1

**TRIBAL GAMING PROGRAM**

Commodities

Tribal Gaming Fund	FY19	FY20	FY21	FY22
	Actual	Actual	Estimate	Estimate
Maintenance Materials, Supplies, Parts	152	87	450	450
Motor Vehicle Parts, Supplies	7,524	4,689	14,500	14,500
Professional & Scientific Supplies	156	209	1,100	1,100
Stationary & Office Supplies	4,218	2,612	4,800	4,800
Other Supplies, Materials, Parts	1,969	957	4,000	4,000
<b>Total Commodities</b>	<b>14,019</b>	<b>8,554</b>	<b>24,850</b>	<b>24,850</b>

Prior Year FY 2020

In FY 19, Commodities were approximately 65.58% below the legislative approved budget. The tribes are given a credit for the amounts below the budget to the current year's assessments.

Current Year FY 2021

In the current year, the commodities budget remains consistent with the FY 20 legislative approved budgeted amount.

Budget Year FY 2022

In the budget year FY 22, the commodities budget remains consistent with the current year budget. Anticipated expenses were obtained through use of historical data, expected variations and executive direction.

Enhancement

There are no commodities enhancements for the Tribal Gaming Program in the budget year.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553 FUNCTION NO. 1  
 PROGRAM TITLE AND CODE Tribal Gaming Program - 03700  
 SUBPROGRAM TITLE AND CODE

**TRIBAL GAMING PROGRAM**

Capital Outlay

**Tribal Gaming Fund**

	<b>FY19</b>	<b>FY20</b>	<b>FY21</b>	<b>FY22</b>
	<b>Actual</b>	<b>Actual</b>	<b>Estimate</b>	<b>Estimate</b>
Vehicles	17,136	17,069	-	-
Equipment, Machinery, Furniture and Fixtures	298	-	1,550	1,550
Professional and Scientific Equipment	-	203	-	-
Books and Library Materials	45	-	300	300
Microcomputer Systems and Support Equipment	9,340	418	10,000	10,000
Information Processing Equipment	15,771	10,104	15,000	15,000
Computer Systems, Info Processing or Micro Software	-	1,325	2,500	2,500
Buildings & Improvements	-	-	-	-
Telecommunications/ Data Facilities	-	-	-	-
	<u>42,590</u>	<u>29,119</u>	<u>29,350</u>	<u>29,350</u>

Prior Year FY 2020

In the prior year, capital outlay was approximately 0.79% below the approved legislative budgeted amount.

Current Year FY 2021

In the current year, the capital outlay budget remains consistent with the FY 20 legislative approved budgeted amount.

Budget Year FY 2022

In the budget year FY22, the capital outlay budget remains consistent with the current year budget.

Anticipated expenses were obtained through use of historical data, expected variations and executive direction.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Expanded Gaming Regulation - 03800
SUBPROGRAM TITLE AND CODE	

**EXPANDED LOTTERY ACT REGULATION PROGRAM (GAMING)**

The KRGC provides regulatory oversight of lottery and racetrack gaming facility managers and their operations in Kansas. Currently, no racetrack gaming facility managers are licensed in Kansas.

**PROGRAM'S STATUTORY HISTORY:**

Under KELA, the State of Kansas is authorized to contract with entities to operate casino-style games owned by the Kansas Lottery Commission. KELA established four gaming zones where lottery gaming facilities could be located and exclusively operated. Additionally, KELA provided that the Kansas Lottery Commission was authorized to contract with racetrack gaming facility managers in three of the four gaming zones to operate slots machines at pari-mutuel facilities.

K.S.A. 74-8772 requires the KRGC to establish and enforce rules and regulations that include but are not limited to: 1) promoting the integrity of gaming and the finances of gaming activity in Kansas that meet or exceed industry standards for monitoring and controlling lottery and racetrack gaming facility managers; 2) prescribing the on-site security at lottery and racetrack gaming facility enterprises in Kansas; 3) reporting of information concerning lottery and racetrack facility managers, their employees, vendors and vendor finances necessary or desirable to ensure the security of lottery or racetrack gaming facility operations; and 4) reporting and auditing of the financial information of lottery or racetrack gaming facility managers, and other information the KRGC requires to determine compliance with KELA and KRGC rules and regulations. KRGC rules and regulations shall include but not be limited to oversight provisions related to: 1) internal controls; 2) security of facilities; 3) performance of background investigations; 4) determination of qualifications and credentialing of employees, contractors and agents of lottery or racetrack gaming facility managers, ancillary lottery gaming facility operations and racetrack gaming facilities; 5) auditing of lottery gaming facility revenue and racetrack gaming facility slot machine income; 6) enforcement of all state laws; and 7) maintaining of the integrity of lottery and racetrack gaming facility operations.

K.S.A. 74-8769 requires that each person subject to a background check under KELA shall be subject to a state and national criminal history records check that conforms to federal standards for the purpose of verifying an applicant's identity and determining whether the applicant has been convicted of any crime that would disqualify the applicant from engaging in activities at lottery or racetrack gaming facilities or ancillary lottery gaming facilities.

K.S.A. 74-8710(a)(13)(B) states that the Kansas Lottery Commission must issue rules and regulations to enforce management contract provisions that require lottery and racetrack gaming facility managers to provide a program to alleviate problem gambling including a requirement that each lottery and racetrack gaming facility maintain a self-exclusion list by which individuals may exclude themselves from access to slots machines and other lottery facility games. Under K.S.A. 74-8772, the KRGC issues rules and regulations to provide regulatory oversight of these management contract provisions that include responsible gambling and voluntary exclusion programs.

K.S.A. 74-8750(c) requires the KRGC to collect from any manufacturer, supplier, provider, lottery gaming facility manager, racetrack gaming facility manager or other person the anticipated actual costs in advance for the examination and certification of electronic gaming machines or lottery facility games. KRGC will reimburse any overpayment and collect any under payment from the appropriate vendor.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553  
 PROGRAM TITLE AND CODE Expanded Gaming Regulation - 03800  
 SUBPROGRAM TITLE AND CODE

**EXPANDED LOTTERY ACT REGULATION PROGRAM (GAMING)**

**Key Performance Measures**

	<b>Actual FY 2015</b>	<b>Actual FY 2016</b>	<b>Actual FY 2017</b>	<b>Actual FY 2018</b>	<b>Actual FY 2019</b>	<b>Actual FY 2020</b>	<b>Estimate FY 2021</b>	<b>Estimate FY 2022</b>
Number of background investigations completed (individual & corporate)	1,214	988	1,155	1,199	1,123	927	1,260	1,260
Percentage of employee licenses denied by the Commission	2%	2%	1%	1%	1%	1%	2%	2%
Number of initial EGM inspections/certifications	1,002	871	811	707	791	375	500	500
Number of Criminal Case Reports	233	348	415	521	486	409	356	450
Illegal gaming machines seized (# does not include components, prizes and other related items seized)	12	17	18	14	47	39	50	50
Illegal gambling complaints received	84	132	82	155	176	143	157	160
Local criminal prosecutions initiated with KRGC assistance*	0	59	13	0	1	0	1	2
Number of VEP enrollees granted access to lottery gaming facility	54	81	59	112	85	86	95	95
Number of new Voluntary Exclusion Program enrollments	268	289	273	273	289	200	287	287

\* Includes prosecutions where KRGC was appointed special counsel to prosecute as well as those where KRGC provided education, guidance, technical expertise, etc. to county or district attorneys that resulted in initiation of prosecutions.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553  
 PROGRAM TITLE AND CODE Expanded Gaming Regulation - 03800  
 SUBPROGRAM TITLE AND CODE Gaming Regulation

DIVISION OF THE BUDGET  
 STATE OF KANSAS

**EXPANDED LOTTERY ACT REGULATION PROGRAM (GAMING)**  
*Subprogram Gaming Regulation*

**Purpose:**

Uphold and promote the integrity of gaming at lottery and racetrack gaming facilities. Ensure the state of Kansas is receiving its fair share of gaming revenue and patrons are receiving the gaming experience according to state law. Ensure compliance with KRGC rules and regulations and applicable state and federal laws.

**Required By Statute:** Yes.

**Maintenance of Effort or Matching Requirement:** None.

**Statutory Requirements:** K.S.A. 74-8733 through 74-8773.

**Consequences of Not Funding:** State-owned gaming facilities would not report to a regulatory body and may not operate in a manner that promotes and upholds the integrity of gaming.

**PROGRAM GOALS - INTEGRITY OF GAMING**

Uphold and promote the integrity of gaming at lottery and racetrack gaming facilities.

Protect gaming operations from the influence of individuals or entities seeking to harm the integrity of gaming in Kansas.

Protect the state of Kansas and its citizens from criminal activity and other potential issues related to the operation of lottery and racetrack gaming facilities.

**Objectives**

Conduct timely and thorough background investigations on all gaming licensees required by KELA.

Investigate complaints and alleged violations of the KRGC rules and regulations and state law related to the lottery and racetrack gaming facilities.

Prohibit ineligible applicants from obtaining licenses and access to casino facilities and activities.

**OUTCOME MEASURE:**

	Actual FY 2015	Actual FY 2016	Actual FY 2017	Actual FY 2018	Actual FY 2019	Actual FY 2020	Estimate FY 2021	Estimate FY 2022
Corporate Background Completion %	120%	84%	94%	83%	136%	150%	95%	95%
Individual Background Completion %	93%	86%	71%	102%	69%	91%	95%	95%
% of Employee Applicants Denied Temporary Permits	8%	11%	6%	4%	3%	2%	5%	5%
% Employee Licenses Denied by Commission	2%	2%	1%	1%	1%	1%	2%	2%
Licenses revoked because of previously undiscovered information	0%	0%	0%	0%	0%	0%	0%	0%

**OUTPUT MEASURES:**

Corporate Background Investigations:	Completed	37	19	11	5	16	6	10	10
	Pending/In-Process	27	29	24	29	35	63	20	20
	Updates/Renewals	11	8	20	26	18	26	20	20
Individual Background Investigations:	Completed	1,177	969	1,144	1,194	1,107	921	1,250	1,250
	Pending/In-Process	423	608	900	707	987	686	750	750
	Updates/Renewals	893	1,031	939	1,252	1,037	1,031	1,250	1,250
Vendor Licenses:	Approved	37	19	11	5	15	6	15	15
	Temporary	12	9	5	6	6	2	10	10
	Renewals	11	8	20	26	18	26	20	20
Casino Employee Licenses:	Gaming Licenses Approved	683	639	705	896	691	635	800	800
	Gaming Licenses Denied	16	21	22	25	16	18	20	20
	Temporary Work Permits Issues	685	689	908	698	837	555	800	800
	License Renewals	702	744	623	827	704	695	750	750
Criminal Case Reports	233	348	415	521	486	409	356	450	

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Expanded Gaming Regulation - 03800
SUBPROGRAM TITLE	Gaming Regulation

**EXPANDED LOTTERY ACT REGULATION PROGRAM (GAMING)**  
*Subprogram Gaming Regulation Continued*

**PROGRAM GOALS - ACCOUNTABILITY & COMPLIANCE**

Uphold and promote the integrity of gaming at lottery and racetrack gaming facilities.  
Ensure the state of Kansas is receiving its fair share of gaming revenue and patrons are receiving the gaming experience according to state law.  
Ensure compliance with KRGC rules and regulations and applicable state and federal laws.

**Objectives**

- Certify all electronic gaming machines (EGM) and systems that will be used at lottery and racetrack gaming facilities in the State of Kansas.
- Audit the collection of net gaming revenue.
- Collect and analyze daily information on bets, wins, tickets, jackpots and drops from slots and daily table game totals.
- Audit net gaming revenue by analyzing daily billings from the Lottery's central computer system and comparing it to each casino's management system.
- Analyze reports on jackpot tax reporting, comps, e-promo's and customer deposits.
- Audit the internal controls and procedures of each lottery gaming facility to ensure compliance with regulations and standards for operations.
- Investigate complaints and alleged violations of the KRGC rules and regulations and applicable state and federal laws.

**OUTCOME MEASURES:**

	Actual FY 2015	Actual FY 2016	Actual FY 2017	Actual FY 2018	Actual FY 2019	Actual FY 2020	Estimate FY 2021	Estimate FY 2022
Improper gaming outcome discovered after complaint	2	0	1	0	0	0	0	0
Improper payment to the state discovered after audit	0	0	0	0	0	0	0	0
Casino internal audits completed within allotted time	100%	100%	100%	100%	100%	100%	100%	100%
Customer Complaints Investigated	100%	100%	100%	100%	100%	100%	100%	100%
KRGC Responses to Customer Complaints	100%	100%	100%	100%	100%	100%	100%	100%

**OUTPUT MEASURES:**

EGM Disputes Investigated	5	2	4	15	17	17	15	15
Machine Software Inspections	2,061	1,780	3,244	1,693	1,913	2,280	2,000	2,000
Initial EGM Inspections/Certifications	1,002	871	811	707	791	375	500	500
EGM Hardware/Software Components Tested and Approved	2,413	2,373	2,371	2,359	2,634	2,683	2,600	2,600
Table Games Tested and Approved	1	3	12	4	27	3	8	8
Internal Control Plans Approved	0	0	1	0	0	0	0	0
Internal Control Plan Amendments Reviewed	102	60	103	105	77	60	80	80
Internal Control Plan Amendments Approved	82	46	75	95	66	55	70	70
Investigations of Variances/Findings found in Audits	12	13	0	0	0	2	1	1
Security Plans Approved	0	0	1	0	0	0	0	0
Security Plan Amendments Reviewed	2	2	2	3	1	2	1	1
Security Plan Amendments Approved	2	2	2	1	2	2	2	2
Non-Criminal Incident Reports	498	350	642	523	492	807	703	890
Official Customer Complaints Received	9	5	4	5	10	14	9	9

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Expanded Gaming Regulation - 03800
SUBPROGRAM TITLE AND CODE	Illegal Gaming

**EXPANDED LOTTERY ACT REGULATION PROGRAM (GAMING)**

*Subprogram Illegal Gaming*

**Purpose:**

Protect the state of Kansas and its citizens from unregulated gaming.

**Required By Statute:** Yes.

**Maintenance of Effort or Matching Requirement:** None.

**Statutory Requirements:** 74-8750(b)&(d); 74-8772(e); Appropriations language establishes the illegal gambling fund for machines seized through enforcement by KRGC.

**Consequences of Not Funding:** Failure to fund could result in the proliferation of gaming that is corrupt. It can also impact the gaming revenue the State receives.

**PROGRAM GOAL - ILLEGAL GAMING ENFORCEMENT**

Coordinate with state agencies and local authorities to reduce and minimize illegal gaming in Kansas.

**Objectives**

- Respond to inquiries and educate the public about illegal gambling.
- Seek voluntary compliance from any business or individual in the state against whom there is an illegal gambling complaint.
- Remove illegal gambling devices from public use through civil seizure and forfeiture when voluntary compliance is not possible.
- Coordinate with local authorities to litigate issues that cannot be achieved through voluntary compliance or civil seizure.

	Actual FY 2015	Actual FY 2016	Actual FY 2017	Actual FY 2018	Actual FY 2019	Actual FY 2020	Estimate FY 2021	Estimate FY 2022
<b><u>OUTPUT MEASURES:</u></b>								
Illegal gaming machines seized (# does not include components, prizes and other related items seized)	12	17	18	14	47	39	50	50
Illegal gambling complaints received	84	132	82	155	176	143	157	160
Local criminal prosecutions initiated with KRGC assistance*	0	59	13	0	1	0	1	2

\* Includes prosecutions where KRGC was appointed special counsel to prosecute as well as those where KRGC provided education, guidance, technical expertise, etc. to county or district attorneys that resulted in initiation of prosecutions.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Expanded Gaming Regulation - 03800
SUBPROGRAM TITLE AND CODE	Responsible Gaming

**EXPANDED LOTTERY ACT REGULATION PROGRAM (GAMING)**

*Subprogram Responsible Gaming*

**Purpose:**

Facilitate responsible gaming in the State of Kansas by administering the voluntary exclusion program.

**Required By Statute:** Yes.

**Maintenance of Effort or** None.  
**Matching Requirement:**

**Statutory Requirements:** K.S.A. 74-8733 through 74-8773.

**Consequences of Not Funding:** There would be no voluntary exclusion program for problem gamblers to sign up for and there would no longer be a state-wide mechanism to prevent problem gamblers from legally entering a State-owned casino.

**PROGRAM GOAL - RESPONSIBLE GAMBLING**

Promote responsible gambling in the state of Kansas.

**Objectives**

- Administer the Voluntary Exclusion Program (VEP).
- Audit and approve each lottery gaming facility's responsible gambling plan for KRGC regulatory compliance.
- Ensure all lottery gaming facility advertising satisfies KRGC regulations.

	<b>Actual FY 2015</b>	<b>Actual FY 2016</b>	<b>Actual FY 2017</b>	<b>Actual FY 2018</b>	<b>Actual FY 2019</b>	<b>Actual FY 2020</b>	<b>Estimate FY 2021</b>	<b>Estimate FY 2022</b>
<b><u>OUTCOME MEASURE:</u></b>								
Number of VEP enrollees granted access to lottery gaming facility	54	81	59	112	85	86	95	95
Number of audit deficiencies of lottery gaming facility's responsible gambling plan (initiated FY 2013)	2	0	0	0	0	0	0	0
Number of problem gambling helpline calls reporting lottery gaming facility as source (% of total)	22%	18%	25%	16%	15%	14%	15%	15%
<b><u>OUTPUT MEASURES:</u></b>								
Number of new Voluntary Exclusion Program enrollments	268	289	273	273	289	200	287	287

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME Kansas Racing and Gaming Commission  
AGENCY NUMBER 553  
PROGRAM TITLE AND CODE Expanded Gaming Regulation - 03800  
SUBPROGRAM TITLE AND CODE

**EXPANDED GAMING REGULATION PROGRAM**

Salaries and Wages

	FY12 Actual	FY13 Actual	FY14 Actual	FY15 Actual	FY16 Actual	FY17 Actual	FY18 Actual	FY19 Actual	FY20 Actual	FY21 Estimate	FY22 Estimate
<b>Gaming Regulation Sub-Program - 03861</b>											
Expanded Lottery Act Regulation Fund	3,776,165	4,299,002	3,939,694	3,967,373	3,987,843	4,425,473	4,784,630	4,960,509	5,151,087	5,963,858	6,023,374
Gaming Background Investigations Fund	241,985	302,797	296,022	235,606	205,429	167,533	170,982	201,735	179,014	295,721	298,709
<b>Subtotal Salaries and Wages - 03861</b>	<b>4,018,150</b>	<b>4,601,799</b>	<b>4,235,716</b>	<b>4,202,979</b>	<b>4,193,272</b>	<b>4,593,006</b>	<b>4,955,612</b>	<b>5,162,244</b>	<b>5,330,101</b>	<b>6,259,579</b>	<b>6,322,083</b>
<b>Responsible Gaming Sub-Program - 03862</b>											
Expanded Lottery Act Regulation Fund	-	-	-	-	-	-	2,031	39,597	30,882	27,228	27,480
Gaming Background Investigations Fund	-	-	-	-	-	-	-	-	-	-	-
<b>Subtotal Salaries and Wages - 03862</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>2,031</b>	<b>39,597</b>	<b>30,882</b>	<b>27,228</b>	<b>27,480</b>
<b>Illegal Gaming Sub-Program - 03863</b>											
Expanded Lottery Act Regulation Fund	-	-	-	-	-	81,429	81,429	76,611	82,557	150,233	151,625
Gaming Background Investigations Fund	-	-	-	-	-	-	-	-	-	-	-
<b>Subtotal Salaries and Wages - 03863</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>81,429</b>	<b>81,429</b>	<b>76,611</b>	<b>82,557</b>	<b>150,233</b>	<b>151,625</b>
<b>Total Salaries and Wages - Expanded Gaming Regulation Program</b>	<b>4,018,150</b>	<b>4,601,799</b>	<b>4,235,716</b>	<b>4,202,979</b>	<b>4,193,272</b>	<b>4,674,435</b>	<b>5,039,072</b>	<b>5,278,452</b>	<b>5,443,540</b>	<b>6,437,040</b>	<b>6,501,188</b>

Prior Year -FY 2020

Salaries for the prior year were for the KRGC's employees at the central office in Topeka, the Boot Hill Casino in Dodge City, the Kansas Star Casino in Mulvane, the Hollywood Casino at the Kansas Speedway in Wyandotte county, and the Kansas Crossing Casino in Crawford county. The KRGC had an approved FTE limit of 86.5. The FTEs consist of 11 regular classified positions and 75.5 regular unclassified positions. In addition, KRGC has 5 commissioners which are non-FTE temporary unclassified.

Current Year FY 2021

Salaries and wages for FY 2021 are for the KRGC employees that regulate gaming from the central office in Topeka, the Boot Hill Casino, the Kansas Star Casino, the Hollywood Casino, and the Kansas Crossing Casino. The KRGC has an approved FTE limit of 86.5 FTE positions for FY 2021. In addition, the KRGC funds a 0.5 temporary unclassified position, 5 KRGC Commissioners in the temporary unclassified service. KRGC has not revised its requested FTE from the approved FY 2021 budget. KRGC has assumed a shrinkage of 5% which is about \$340,000.

Budget Year FY 2022

Salaries and wages for FY 2022 are for the KRGC employees that regulate gaming from the central office in Topeka, the Boot Hill Casino, the Kansas Star Casino, the Hollywood Casino, and the Kansas Crossing Casino. The KRGC has an approved FTE limit of 86.5 FTE positions for FY 2021. In addition, the KRGC funds a 0.5 temporary unclassified position, 5 KRGC Commissioners in the temporary unclassified service. KRGC has not revised its requested FTE from the approved FY 2021 budget. KRGC has assumed a shrinkage of 5% which is about \$342,000.

Current Year FY 2021- Supplemental

There is no supplemental package for FY 2021.

Budget Year FY 2022- Supplemental

There is no supplemental package for FY 2022.

**NARRATIVE INFORMATION -- DA 400**

Kansas Racing and Gaming Commission

553

DIVISION OF THE BUDGET  
STATE OF KANSAS

Expanded Gaming Regulation - 03800

**EXPANDED GAMING REGULATION PROGRAM**

**Contractual Services**

**Contractual Services by Sub-Program**

	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21	FY22
	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Estimate	Estimate
<b>Gaming Regulation Sub-Program - 03861</b>										
<b>Expanded Lottery Act Reg Fund - 2535</b>										
Communication	76,940	78,720	82,125	92,329	93,861	79,494	62,571	64,043	85,200	85,200
Freight & Express	548	742	617	1,082	1,407	4,490	4,008	3,488	1,300	1,300
Printing & Advertising	1,783	381	563	369	-	-	45	842	1,450	1,450
Rents	175,499	169,506	169,348	213,241	208,953	215,597	232,254	223,794	240,650	240,650
Repairing & Servicing	41,266	41,778	60,331	21,446	49,537	20,846	20,901	109,664	55,708	55,708
Travel & Subsistence	89,379	92,228	72,594	75,822	121,777	89,902	67,729	75,366	151,634	151,634
Fees - Other Services	291,070	245,033	249,376	251,126	312,416	350,094	349,065	247,461	316,940	316,940
Fees - Professional Services	8,125	56,068	538,272	9,024	6,614	28,743	51,841	69,247	82,050	82,050
Other Contractual Services	3,485	1,008	11,298	3,936	4,820	4,123	2,675	3,026	19,043	19,043
<b>Subtotal - Cont. Services - ELARF</b>	<b>688,095</b>	<b>685,564</b>	<b>1,184,524</b>	<b>668,375</b>	<b>799,385</b>	<b>793,289</b>	<b>791,089</b>	<b>796,931</b>	<b>953,975</b>	<b>953,975</b>
<b>Gaming Background Investigations Fund - 2682</b>										
Communication	-	-	-	-	-	-	-	-	-	-
Freight & Express	65	-	104	-	-	-	-	-	-	-
Printing & Advertising	-	-	-	-	-	-	-	-	-	-
Rents	-	-	-	-	-	-	-	-	-	-
Repairing & Servicing	-	-	-	-	-	-	-	-	-	-
Travel & Subsistence	34,791	39,701	31,478	31,478	9,645	12,996	14,377	6,019	35,250	35,250
Fees - Other Services	2,239	10,000	22	22	-	5	321	142	-	-
Fees - Professional Services	-	-	-	-	-	-	-	-	-	-
Other Contractual Services	-	-	-	-	-	-	-	-	-	-
<b>Subtotal - Cont. Services - Gaming Background Invest. Fund</b>	<b>37,095</b>	<b>49,701</b>	<b>31,604</b>	<b>31,500</b>	<b>9,645</b>	<b>13,001</b>	<b>14,698</b>	<b>6,161</b>	<b>35,250</b>	<b>35,250</b>
<b>Illegal Gambling Enforcement Fund - 2734</b>										
Communication	-	-	-	-	-	-	-	-	-	-
Freight & Express	-	-	-	-	-	-	-	-	-	-
Printing & Advertising	-	-	-	-	-	-	-	-	-	-
Rents	-	-	-	-	-	-	-	-	-	-
Repairing & Servicing	-	-	-	-	-	-	-	-	-	-
Travel & Subsistence	-	-	-	-	-	-	-	-	-	-
Fees - Other Services	-	-	-	-	-	-	-	-	-	-
Fees - Professional Services	-	-	-	-	-	-	-	-	-	-
Other Contractual Services	-	-	-	-	-	-	-	-	-	-
<b>Subtotal - Cont. Services - Illegal Gambling Enforcement Fund</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Subtotal - Cont. Services - Gaming Regulation 03861</b>	<b>725,190</b>	<b>735,265</b>	<b>1,216,128</b>	<b>699,875</b>	<b>809,030</b>	<b>806,290</b>	<b>805,787</b>	<b>803,092</b>	<b>989,225</b>	<b>989,225</b>
<b>Responsible Gaming Sub-Program - 03862</b>										
<b>Expanded Lottery Act Regulation Fund - 2535</b>										
Communication	-	-	-	-	-	-	-	-	-	-
Freight & Express	-	-	-	-	-	-	-	-	-	-
Printing & Advertising	-	-	-	-	-	-	-	-	-	-
Rents	-	-	-	-	-	-	-	-	-	-
Repairing & Servicing	-	-	-	-	-	-	-	-	-	-
Travel & Subsistence	-	-	-	-	-	-	-	-	-	-
Fees - Other Services	-	-	-	-	-	-	-	-	-	-
Fees - Professional Services	-	-	-	-	-	-	-	-	-	-
Other Contractual Services	-	-	-	-	-	-	-	-	-	-
<b>Subtotal - Cont. Services - ELARF</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Gaming Background Investigations Fund</b>										
Communication	-	-	-	-	-	-	-	-	-	-
Freight & Express	-	-	-	-	-	-	-	-	-	-
Printing & Advertising	-	-	-	-	-	-	-	-	-	-
Rents	-	-	-	-	-	-	-	-	-	-
Repairing & Servicing	-	-	-	-	-	-	-	-	-	-
Travel & Subsistence	-	-	-	-	-	-	-	-	-	-
Fees - Other Services	-	-	-	-	-	-	-	-	-	-
Fees - Professional Services	-	-	-	-	-	-	-	-	-	-
Other Contractual Services	-	-	-	-	-	-	-	-	-	-
<b>Subtotal - Cont. Services - Gaming Background Invest. Fund</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Illegal Gambling Enforcement Fund - 2734</b>										
Communication	-	-	-	-	-	-	-	-	-	-
Freight & Express	-	-	-	-	-	-	-	-	-	-
Printing & Advertising	-	-	-	-	-	-	-	-	-	-
Rents	-	-	-	-	-	-	-	-	-	-
Repairing & Servicing	-	-	-	-	-	-	-	-	-	-
Travel & Subsistence	-	-	-	-	-	-	-	-	-	-
Fees - Other Services	-	-	-	-	-	-	-	-	-	-
Fees - Professional Services	-	-	-	-	-	-	-	-	-	-
Other Contractual Services	-	-	-	-	-	-	-	-	-	-
<b>Subtotal - Cont. Services - Illegal Gambling Enforcement Fund</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Subtotal Cont. Services - Responsible Gambling 03862</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Illegal Gaming Sub-Program - 03863</b>										
<b>Expanded Lottery Act Reg Fund - 2535</b>										
Communication	-	-	-	-	-	-	-	-	-	-
Freight & Express	-	-	-	-	-	-	-	-	-	-
Printing & Advertising	-	-	-	-	-	-	-	-	-	-
Rents	-	-	-	-	-	-	-	200	-	-
Repairing & Servicing	-	-	-	-	-	-	-	-	-	-
Travel & Subsistence	-	-	-	-	-	150	198	477	-	-
Fees - Other Services	-	-	-	-	-	-	15	-	-	-
Fees - Professional Services	-	-	-	-	-	-	-	-	-	-
Other Contractual Services	-	-	-	-	-	-	-	-	-	-
<b>Subtotal - Cont. Services - ELARF</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>150</b>	<b>213</b>	<b>677</b>	<b>-</b>	<b>-</b>
<b>Illegal Gambling Enforcement Fund - 2734</b>										
Communication	-	-	-	-	-	-	240	-	-	-
Freight & Express	-	-	-	-	-	-	-	-	-	-
Printing & Advertising	-	-	-	-	-	-	-	-	-	-
Rents	-	-	-	-	178	-	-	780	-	-
Repairing & Servicing	-	-	-	-	-	-	-	70	-	-
Travel & Subsistence	-	-	-	-	726	207	1,206	-	-	-
Fees - Other Services	-	-	-	-	-	408	145	-	-	-
Fees - Professional Services	-	-	828	292	-	-	-	-	-	-
Other Contractual Services	110	2,839	-	1,367	107	-	221	116	3,000	3,000
<b>Subtotal - Cont. Services - Illegal Gambling Enforcement Fund</b>	<b>110</b>	<b>2,839</b>	<b>828</b>	<b>1,659</b>	<b>1,011</b>	<b>615</b>	<b>1,312</b>	<b>866</b>	<b>3,000</b>	<b>3,000</b>
<b>Subtotal - Cont. Services - Illegal Gaming 03863</b>	<b>110</b>	<b>2,839</b>	<b>828</b>	<b>1,659</b>	<b>1,011</b>	<b>765</b>	<b>2,025</b>	<b>1,643</b>	<b>3,000</b>	<b>3,000</b>
<b>Total Contractual Services - Expanded Gaming Regulation Program</b>	<b>725,300</b>	<b>738,104</b>	<b>1,216,956</b>	<b>701,534</b>	<b>810,041</b>	<b>807,055</b>	<b>807,812</b>	<b>804,735</b>	<b>992,225</b>	<b>992,225</b>

**Prior Year - FY 2020**

The majority of contractual expenditures for FY 2020 are for the regulation of the four lottery gaming facilities currently operating. Expenses for central administration primarily consist of rent and monument charge (\$208,000), and fees related to background investigations (\$147,000).

**Current Year - FY 2021**

FY 2021 contractual services include expenditures for ongoing operations associated with the regulation of the Boot Hill Casino in Dodge City, the Hollywood Casino in Wyandotte county, the Kansas Star Casino near Mulvane, and The Kansas Crossing Casino in Pittsburg. Travel and subsistence is for performing internal control audits at gaming facilities; voluntary exclusion program audits; electronic gaming equipment and security audits; background investigations of casino employees; agent and employee training; travel for the Commission; fees and professional services largely consisting of database access fees (i.e. KBI database) related to background checks for gaming facility employees. The majority of rental cost is Topco office space and monument charge in the Eisenhower State Office Building. Costs from the Gaming Background Investigations fund are related to background checks of vendors who are providing goods and services to the gaming facilities.

NOTE: The KRGC requests to continue the Hospitality Fund in the amount of \$1,500 for purpose of hosting public meetings.

**Enhancement - FY 2021**

There are no contractual service enhancements for the Kansas Racing and Gaming Commission in the budget year.

**NARRATIVE INFORMATION -- DA 400**

Kansas Racing and Gaming Commission

553

Expanded Gaming Regulation - 03800

DIVISION OF THE BUDGET  
STATE OF KANSAS

**EXPANDED GAMING REGULATION PROGRAM**

**Contractual Services (Continued)**

**Budget Year - FY 2022**

The FY 2022 budget year reflects costs for the ongoing expanded gaming regulation of the four operational lottery gaming facilities and is virtually identical to the approved FY 2021 contractual services budget.

NOTE: The KRGC requests to continue the Hospitality Fund in the amount of \$1,500 for purpose of hosting public meetings.

**Enhancement - FY 2022**

There are no contractual service enhancements for the Kansas Racing and Gaming Commission in the FY 2022 budget.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553  
 PROGRAM TITLE AND CODE Expanded Gaming Regulation - 03800  
 SUBPROGRAM TITLE AND CODE

DIVISION OF THE BUDGET  
 STATE OF KANSAS

**EXPANDED GAMING REGULATION PROGRAM**

Commodities

**Commodities by Sub-Program**

	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21	FY22
	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Estimate	Estimate
<b>Gaming Regulation Sub-Program - 03861</b>										
<b>Expanded Lottery Act Reg Fund -2535</b>										
Clothing	-	-	-	2,952	1,550	13	3,928	11,131	-	-
Food	-	-	16	155	16	55	32	514	-	-
Maintenance Materials, Supplies, Parts	1,082	762	1,536	1,992	3,395	8,215	3,891	7,694	4,100	4,100
Motor Vehicle Parts, Supplies	9,866	8,317	7,064	6,476	9,356	7,453	10,967	-	28,055	28,055
Professional & Scientific Supplies	4,242	13,408	578	1,005	421	4,061	793	3,535	25,860	25,860
Stationary & Office Supplies	28,220	30,106	26,925	22,996	48,872	10,933	21,312	13,828	74,555	74,555
Other Supplies, Materials, Parts	7,439	6,255	6,355	33,658	43,710	34,087	24,036	9,671	4,300	4,300
<b>Subtotal - Commodities - ELARF</b>	<b>50,850</b>	<b>58,848</b>	<b>42,474</b>	<b>69,234</b>	<b>107,320</b>	<b>64,817</b>	<b>64,959</b>	<b>46,373</b>	<b>136,870</b>	<b>136,870</b>
<b>Gaming Background Investigations Fund - 2682</b>										
Maintenance Materials, Supplies, Parts	-	-	-	-	-	-	-	-	-	-
Motor Vehicle Parts, Supplies	1,080	1,254	1,135	601	201	249	504	-	1,700	1,700
Professional & Scientific Supplies	-	-	-	-	-	-	-	139	-	-
Stationary & Office Supplies	-	-	-	-	-	-	-	-	-	-
Other Supplies and Materials	-	-	45	-	45	-	-	-	-	-
<b>Subtotal - Commodities - Gaming Background Investigations Fund</b>	<b>1,080</b>	<b>1,254</b>	<b>1,180</b>	<b>601</b>	<b>246</b>	<b>249</b>	<b>504</b>	<b>139</b>	<b>1,700</b>	<b>1,700</b>
<b>Illegal Gambling Enforcement Fund - 2734</b>										
<b>Subtotal - Commodities - Illegal Gambling Enforcement Fund</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Subtotal - Commodities - Gaming Regulation</b>	<b>51,929</b>	<b>60,102</b>	<b>43,654</b>	<b>69,835</b>	<b>107,566</b>	<b>65,066</b>	<b>65,463</b>	<b>46,512</b>	<b>138,570</b>	<b>138,570</b>
<b>Responsible Gaming Sub-Program - 03862</b>										
<b>Expanded Lottery Act Regulation Fund - 2535</b>										
<b>Subtotal - Commodities - ELARF</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Gaming Background Investigations Fund</b>										
<b>Subtotal - Commodities - Gaming Background Investigations Fund</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Illegal Gambling Enforcement Fund - 2734</b>										
<b>Subtotal - Commodities - Illegal Gambling Enforcement Fund</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Subtotal Commodities - Responsible Gambling 03862</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
<b>Illegal Gaming Sub-Program - 03863</b>										
<b>Expanded Lottery Act Regulation Fund - 2535</b>										
Maintenance Materials, Supplies, Parts	-	-	-	-	-	-	-	-	-	-
Motor Vehicle Parts, Supplies	1,053	1,015	1,053	434	-	639	371	297	1,200	1,200
Professional & Scientific Supplies	264	-	-	-	574	-	-	-	-	-
Stationary & Office Supplies	-	-	-	-	-	-	-	-	-	-
Other Supplies and Materials	-	-	-	-	-	136	-	207	-	-
<b>Subtotal - Commodities - ELARF</b>	<b>1,317</b>	<b>1,015</b>	<b>1,053</b>	<b>434</b>	<b>574</b>	<b>775</b>	<b>371</b>	<b>504</b>	<b>1,200</b>	<b>1,200</b>
<b>Illegal Gambling Enforcement Fund - 2734</b>										
Maintenance Materials, Supplies, Parts	-	-	-	36	-	-	-	-	-	-
Motor Vehicle Parts, Supplies	-	-	-	-	151	722	580	238	-	-
Professional & Scientific Supplies	-	-	-	788	574	-	-	-	-	-
Stationary & Office Supplies	-	-	-	-	-	-	65	240	-	-
Other Supplies and Materials	414	-	-	1,425	-	-	16	-	-	-
<b>Subtotal - Commodities - Illegal Gambling Enforcement Fund</b>	<b>414</b>	<b>-</b>	<b>-</b>	<b>2,249</b>	<b>725</b>	<b>722</b>	<b>661</b>	<b>478</b>	<b>-</b>	<b>-</b>
<b>Subtotal - Commodities - Illegal Gambling - 03863</b>	<b>1,731</b>	<b>1,015</b>	<b>1,053</b>	<b>2,683</b>	<b>1,299</b>	<b>1,497</b>	<b>1,032</b>	<b>982</b>	<b>1,200</b>	<b>1,200</b>
<b>Total Commodities - Expanded Gaming Regulation Program</b>	<b>53,660</b>	<b>61,117</b>	<b>44,707</b>	<b>72,518</b>	<b>108,865</b>	<b>66,563</b>	<b>66,495</b>	<b>47,494</b>	<b>139,770</b>	<b>139,770</b>

**Prior Year - FY 2020**

The FY 2020 reflects costs associated with the regulation of expanded gaming for the Topeka office, the Boot Hill Casino in Ford county, Hollywood Casino in Wyandotte county, Kansas Star Casino in Sumner county, and Kansas Crossing Casino in Crawford county. Major categories of supplies include materials for repair of office equipment; supplies and materials for repair and maintenance of state vehicles (e.g. oil changes, tires) and fuel charges for state vehicles; professional and scientific supplies for law enforcement materials (e.g. hand guns, ammunition, EGM testing supplies), legal directories and security tags for gaming machines; office supplies for the Topeka, Boot Hill Casino, Kansas Star Casino, Hollywood Casino, and Kansas Crossing Casino KRGC offices. Office supplies include security badge supplies for the printing and replacement of security badges for gaming facility employees.

**Current Year - FY 2021**

The FY 2021 commodities budget reflects costs associated with the regulation of expanded gaming for the Topeka, the Boot Hill Casino, the Hollywood Casino, the Kansas Star Casino, and the Kansas Crossing Casino KRGC offices and is unchanged from the FY 2021 approved budget.

**Enhancement - FY 2021**

There are no commodity enhancements for the Kansas Racing and Gaming Commission in the budget year.

**NARRATIVE INFORMATION -- DA 400**

DIVISION OF THE BUDGET  
STATE OF KANSAS

AGENCY NAME	Kansas Racing and Gaming Commission
AGENCY NUMBER	553
PROGRAM TITLE AND CODE	Expanded Gaming Regulation - 03800
SUBPROGRAM TITLE AND CODE	

**EXPANDED GAMING REGULATION PROGRAM**

**Commodities (Continued)**

**Budget Year - FY 2022**

The FY 2022 commodities budget reflects costs associated with the regulation of expanded gaming for the Topeka, the Boot Hill Casino, the Hollywood Casino, the Kansas Star Casino, and the Kansas Crossing Casino KRGC offices and is virtually identical to the approved FY 2021 budget.

**Enhancement - FY 2022**

There are no commodity enhancements for the Kansas Racing and Gaming Commission in the budget year.

**NARRATIVE INFORMATION -- DA 400**

AGENCY NAME Kansas Racing and Gaming Commission  
 AGENCY NUMBER 553  
 PROGRAM TITLE AND CODE Expanded Gaming Regulation - 03800  
 SUBPROGRAM TITLE AND CODE

DIVISION OF THE BUDGET  
 STATE OF KANSAS

**EXPANDED GAMING REGULATION PROGRAM**

Capital Outlay

**Capital Outlay by Sub-Program**

	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21	FY22
	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Estimate	Estimate
<b>Gaming Regulation Sub-Program - 03861</b>										
<b>Expanded Lottery Act Reg Fund - 2535</b>										
Passenger Cars	-	-	-	25,690	65,591	53,246	-	53,240	-	-
Equipment, Machinery, Furniture and Fixtures	931	85	562	15,030	13,058	33,086	5,101	3,428	5,000	20,000
Professional and Scientific Equipment	-	279	11,545	126	19,643	-	239	311	10,000	23,500
Books and Library Materials	290	194	185	-	205	83	-	-	-	-
Microcomputer Systems and Support Equipment	19,426	42,586	35,165	25,253	17,513	17,990	30,427	-	62,000	53,500
Information Processing Equipment	14,351	7,300	8,785	4,562	12,704	8,773	525	44,593	48,300	38,300
Computer Systems, Info Processing or Micro Software	20,830	39,845	30,984	990	42,668	8,318	18,501	-	10,000	-
Telecommunications/ Data Facilities	31,897	-	25	-	1,954	1,749	-	-	-	-
<i>Subtotal - Capital Outlay - ELARF</i>	<b>87,724</b>	<b>90,289</b>	<b>87,251</b>	<b>71,651</b>	<b>173,336</b>	<b>123,245</b>	<b>54,793</b>	<b>101,572</b>	<b>135,300</b>	<b>135,300</b>
<b>Gaming Background Investigations Fund - 2682</b>										
<i>Subtotal - Capital Outlay - Gaming Background Investigations Fund</i>	-	-	-	-	-	-	-	-	-	-
<b>Subtotal - Capital Outlay - 03861</b>	<b>87,724</b>	<b>90,289</b>	<b>87,251</b>	<b>71,651</b>	<b>173,336</b>	<b>123,245</b>	<b>54,793</b>	<b>101,572</b>	<b>135,300</b>	<b>135,300</b>
<b>Responsible Gaming Sub-Program - 03862</b>										
<b>Expanded Lottery Act Reg Fund - 2535</b>										
<i>Subtotal - Capital Outlay - ELARF</i>	-	-	-	-	-	-	-	-	-	-
<b>Gaming Background Investigations Fund - 2682</b>										
<i>Subtotal - Capital Outlay - Gaming Background Investigations Fund</i>	-	-	-	-	-	-	-	-	-	-
<b>Subtotal Capital Outlay - 03862</b>	-	-	-	-	-	-	-	-	-	-
<b>Illegal Gaming Sub-Program - 03863</b>										
<b>Expanded Lottery Act Reg Fund - 2535</b>										
Information Processing Equipment	-	715	-	-	722	42	-	76	-	-
Equipment, Machinery, Furniture and Fixtures	310	-	-	498	-	-	-	-	-	-
<i>Subtotal - Capital Outlay - ELARF</i>	<b>310</b>	<b>715</b>	-	<b>498</b>	<b>722</b>	<b>42</b>	-	<b>76</b>	-	-
<b>Illegal Gambling Enforcement Fund - 2734</b>										
<i>Subtotal - Capital Outlay - Illegal Gambling Fund</i>	-	-	-	-	-	-	-	2,405	-	-
<b>Subtotal Capital Outlay - 03863</b>	<b>310</b>	<b>715</b>	-	<b>498</b>	<b>722</b>	<b>42</b>	-	<b>2,481</b>	-	-
<b>Total Capital Outlay - Expanded Gaming Regulation Program</b>	<b>88,034</b>	<b>91,004</b>	<b>87,251</b>	<b>72,149</b>	<b>174,058</b>	<b>123,287</b>	<b>54,793</b>	<b>104,053</b>	<b>135,300</b>	<b>135,300</b>

**Prior Year - FY2020**

The FY 2020 expenses for capital outlay include replacement of older computer workstations and related software, new work stations and related software the staff in Topeka. Capital outlay purchases also included the renewal of licensing software.

**Current Year - FY 2021**

The FY 2021 budget year reflects continued costs associated with the regulation of gaming for the Topeka office and the KRGC offices located at each of the four lottery gaming facilities. Expenditures include scheduled replacement computer workstations; scheduled server replacement; gaming test equipment; and other miscellaneous hardware. FY 2020 capital outlay budget is unchanged from the approved FY 2021 capital outlay budget.

**Enhancement - FY 2021**

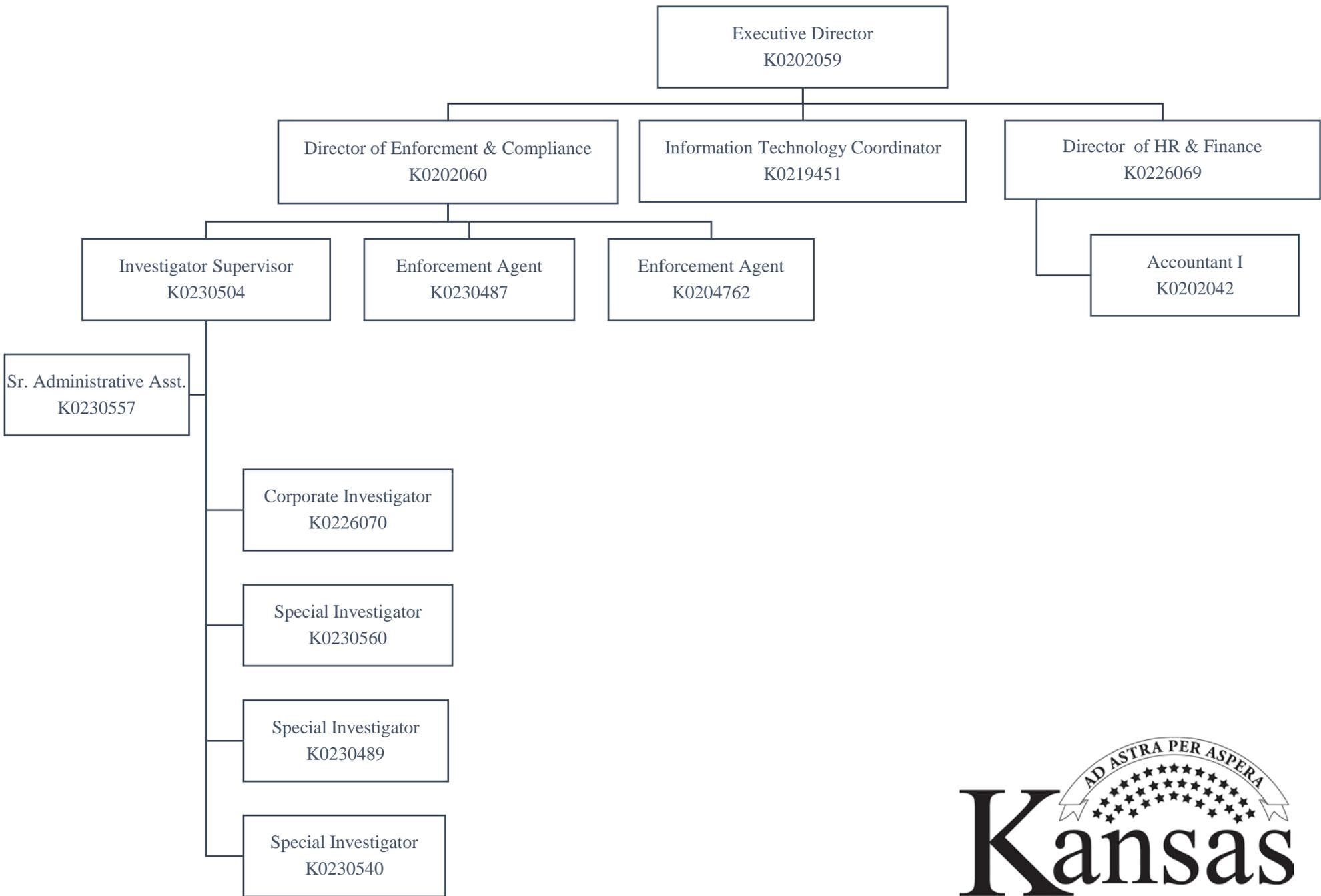
There are no capital outlay enhancements for the Kansas Racing and Gaming Commission in the budget year.

**Budget Year - FY 2022**

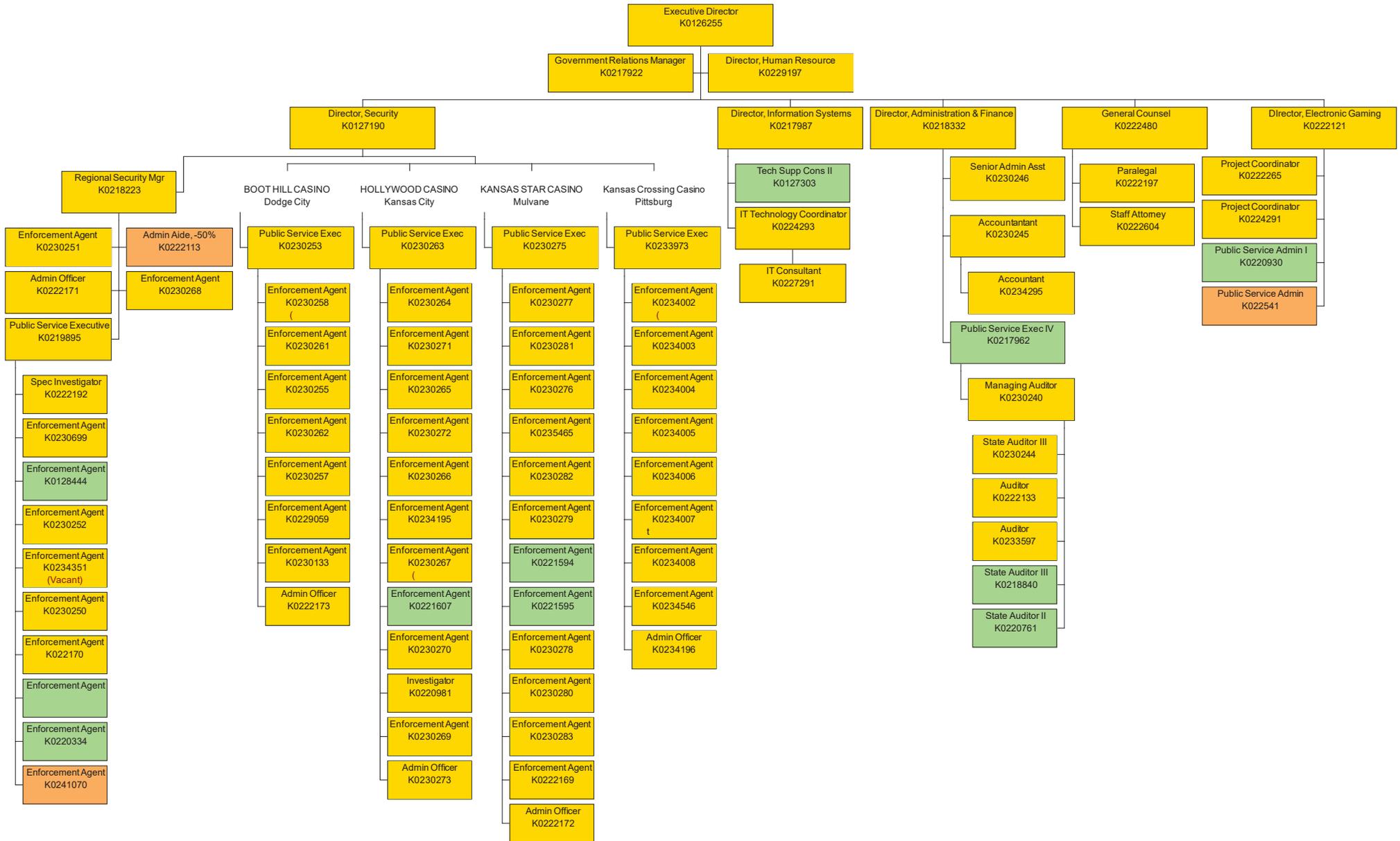
The FY 2022 budget year reflects continued costs associated with the regulation of gaming for the Topeka office and the KRGC offices located at each of the four lottery gaming facilities. Expenditures include scheduled replacement computer workstations; scheduled replacement servers; gaming test equipment; and other miscellaneous hardware. FY 2022 capital outlay budget is virtually identical to the approved FY 2022 capital outlay budget.

**Enhancement - FY 2022**

There are no capital outlay enhancements for the Kansas Racing and Gaming Commission in the budget year.



# Kansas Racing & Gaming Commission



**Kansas Racing and Gaming Commission**

Summary of Expenditures FY 2021 and FY 2022--- Expanded Gaming Program and Parimutuel Program

	<b>FY 2020 Actual</b>	<b>FY 2021 Approved</b>	<b>FY 2021 Revised</b>	<b>Change from FY 2021 Approved</b>	<b>% Change from Approved</b>	<b>FY 2021 Approved</b>	<b>FY 2022 Request</b>	<b>Change from FY 2021 Approved</b>	<b>% Change from Approved</b>
Salaries and Wages		6,888,861	6,779,016	(109,845)	(1.59)	6,888,861	6,846,576	(42,285)	(0.61)
Less Shrinkage		(329,524)	(338,951)	(9,427)	(2.86)	(182,801)	(342,329)	(159,528)	(87.27)
<b>Net Salaries and Wages</b>	<b>5,446,316</b>	<b>6,559,337</b>	<b>6,440,065</b>	<b>(119,272)</b>	<b>(1.82)</b>	<b>6,706,060</b>	<b>6,504,247</b>	<b>(201,813)</b>	<b>(3.01)</b>
<b>Other Operating</b>									
Contractual Services	806,977	993,225	993,225	-	-	993,225	993,225	-	-
Commodities	50,325	139,770	139,770	-	-	139,770	139,770	-	-
Capital Outlay	106,011	135,300	135,300	-	-	135,300	135,300	-	-
<b>Subtotal Other Operating</b>	<b>963,313</b>	<b>1,268,295</b>	<b>1,268,295</b>	<b>-</b>	<b>-</b>	<b>1,268,295</b>	<b>1,268,295</b>	<b>-</b>	<b>-</b>
VRIP and Interest on PMIB	-	-	-	-	-	-	-	-	-
<b>Total Reportable Expense</b>	<b>6,409,629</b>	<b>7,827,632</b>	<b>7,708,360</b>	<b>(119,272)</b>	<b>(1.52)</b>	<b>7,974,355</b>	<b>7,772,542</b>	<b>(201,813)</b>	<b>(2.53)</b>
<b>Non-Reportable Expense:</b>									
Petty Cash Advance	-	-	-	-	-	-	-	-	-
<b>Grand Total Reportable and Non Reportable</b>	<b>6,409,629</b>	<b>7,827,632</b>	<b>7,708,360</b>	<b>(119,272)</b>	<b>(1.52)</b>	<b>7,974,355</b>	<b>7,772,542</b>	<b>(201,813)</b>	<b>(2.53)</b>

Fund Status Summary  
FY 2019 - FY 2022

	FY 2019 Ending Balance	FY 2020 Revenues Actual	FY 2020 Expend Actual	FY 2020 Ending Balance	FY 2021 Revenues Projection	FY 2021 Expend Projection	FY 2021 Ending Balance	FY 2022 Revenues Projection	FY 2022 Expend Projection	FY 2022 Ending Balance
<b>Parimutuel Funds</b>										
2516 - Kansas Horse Breeding Development Fund	51,913	-	-	51,913	-	-	51,913	-	-	51,913
2561 - Greyhound Promotion & Development Fund	-	-	-	-	-	-	-	-	-	-
2601 - Kansas Greyhound Breeding Development Fund	-	-	-	-	-	-	-	-	-	-
5131 - State Racing Fund	69,292	1,723	(1,388)	69,627	1,000	(4,026)	66,601	1,000	(4,060)	63,541
<b>Subtotal</b>	<b>121,205</b>	<b>1,723</b>	<b>(1,388)</b>	<b>121,540</b>	<b>1,000</b>	<b>(4,026)</b>	<b>118,514</b>	<b>1,000</b>	<b>(4,060)</b>	<b>115,454</b>
<b>Gaming Funds</b>										
2535 - Expanded Lottery Act Regulation (Gaming) Fund	3,978,720	4,494,585	(6,219,079)	2,254,226	7,248,381	(7,367,464)	2,135,143	7,075,577	(7,428,624)	1,782,097
2682 - Gaming Background Investigations Fund	270,377	130,155	(185,313)	215,219	250,000	(332,671)	132,548	275,000	(335,659)	71,890
2734- Illegal Gaming Enforcement Fund	14,554	113,908	(3,849)	124,613	5,000	(4,200)	125,413	5,000	(4,200)	126,213
2998- Gaming Machine Examination Fund	-	-	-	-	-	-	-	-	-	-
<b>Subtotal</b>	<b>4,263,651</b>	<b>4,738,648</b>	<b>(6,408,241)</b>	<b>2,594,058</b>	<b>7,503,381</b>	<b>(7,704,334)</b>	<b>2,393,105</b>	<b>7,355,577</b>	<b>(7,768,482)</b>	<b>1,980,199</b>
<b>Total Funds</b>	<b>4,384,856</b>	<b>4,740,371</b>	<b>(6,409,629)</b>	<b>2,715,598</b>	<b>7,504,381</b>	<b>(7,708,360)</b>	<b>2,511,619</b>	<b>7,356,577</b>	<b>(7,772,542)</b>	<b>2,095,654</b>

**Kansas Racing and Gaming Commission**

FTE Summary

FY 2016 - FY 2022

	FY 2016 Actual	FY 2017 Actual	FY 2018 Actual	FY 2019 Approved	FY 2019 Revised	FY 2019 Actual	FY 2020 Approved	FY 2020 Revised	FY 2020 Actual	FY 2021 Approved	FY 2021 Revised	FY 2022 Requested
<b>Central Office</b>												
Executive	5.0	5.0	5.0	6.0	6.0	7.0	7.0	7.0	6.0	7.0	7.0	7.0
Administration and Audit	6.0	8.0	8.0	11.0	11.0	7.0	11.0	11.0	7.0	11.0	11.0	11.0
Animal Health	-	-	-	-	-	-	-	-	-	-	-	-
IT and Electronic Security	7.0	7.0	7.0	9.0	9.0	7.0	8.0	8.0	7.0	8.0	8.0	8.0
Racing	-	-	-	-	-	-	-	-	-	-	-	-
Security & Licensing <sup>1</sup>	10.0	11.0	12.0	15.5	15.5	11.0	15.5	14.5	13.0	15.5	14.5	15.5
<i>Subtotal - Central Office</i>	<i>28.0</i>	<i>31.0</i>	<i>32.0</i>	<i>41.5</i>	<i>41.5</i>	<i>32.0</i>	<i>41.5</i>	<i>40.5</i>	<i>33.0</i>	<i>41.5</i>	<i>40.5</i>	<i>41.5</i>
<b>Facilities</b>												
Wichita Greyhound Park	-	-	-	-	-	-	-	-	-	-	-	-
Woodlands (Kansas City)	-	-	-	-	-	-	-	-	-	-	-	-
Boot Hill (Dodge City)	6.5	6.5	8.5	9.0	9.0	7.0	9.0	9.0	5.0	9.0	9.0	9.0
Sumner Co. Gaming Facility	11.0	11.0	11.0	13.0	13.0	13.0	13.0	14.0	14.0	13.0	14.0	13.0
Hollywood (WY Co.)	13.0	13.0	11.0	13.0	13.0	11.0	13.0	13.0	11.0	13.0	13.0	13.0
Southeast Gaming Zone	-	10.0	9.0	10.0	10.0	9.0	10.0	10.0	9.0	10.0	10.0	10.0
<i>Subtotal - Facilities</i>	<i>30.5</i>	<i>40.5</i>	<i>39.5</i>	<i>45.0</i>	<i>45.0</i>	<i>40.0</i>	<i>45.0</i>	<i>46.0</i>	<i>39.0</i>	<i>45.0</i>	<i>46.0</i>	<i>45.0</i>
<b>Total</b>	<b>58.5</b>	<b>71.5</b>	<b>71.5</b>	<b>86.5</b>	<b>86.5</b>	<b>72.0</b>	<b>86.5</b>	<b>86.5</b>	<b>72.0</b>	<b>86.5</b>	<b>86.5</b>	<b>86.5</b>

Notes

1. Does not include Temporary, Unclassified positions (0.50 Administrative Aide and 5 Commissioners)

**Kansas Racing and Gaming Commission**  
 Budget Worksheet - Receipts  
 FY 2020 - FY 2022

**2535 - Expanded Lottery Act Regulation (Gaming) Fund**

	A	B	C	D	E	F	G	I	J
	FY 2020 Actual	FY 2020 Budget	Difference	FY 2021 Approved Budget	Revisions to FY 2021	Revised FY 2021 Budget	FY 2021 Base Budget	Changes from Revised FY 2021 to FY 2022	Submitted FY 2022 Budget
Receipts									
PMIB Loan Proceeds			-	-	-	-	-	-	-
LGFRB Applicant Reimbursement	-	-	-	-	-	-	-	-	-
SU Start-up Reimbursement	-	-	-	-	-	-	-	-	-
BHRC Start-up Reimb.	-	-	-	-	-	-	-	-	-
WY (Hollywood) Ops Reimbursment	1,368,001	1,950,000	(581,999)	1,950,000	197,829	2,147,829	1,950,000	(74,131)	2,073,698
SU (KC Star) Ops Reimbursment	1,474,782	1,850,000	(375,218)	1,850,000	198,265	2,048,265	1,850,000	198,247	2,246,512
BHRC Ops Reimbursment	732,669	1,050,000	(317,331)	1,050,000	280,903	1,330,903	1,050,000	46,294	1,377,197
Facility Mgr Background Deposits	-	-	-	-	-	-	-	-	-
SE (Southeast) Ops Reimbursement	883,327	1,150,000	(266,673)	1,255,000	466,384	1,721,384	1,255,000	(343,214)	1,378,170
Vendor Background Fees	-	-	-	-	-	-	-	-	-
Miscellaneous Revenue	35,806	-	35,806	-	-	-	-	-	-
ELARF Transfer	-	-	-	-	-	-	-	-	-
Transfer Out	-	-	-	-	-	-	-	-	-
<b>Total Receipts</b>	<b>4,494,585</b>	<b>6,000,000</b>	<b>(1,505,415)</b>	<b>6,105,000</b>	<b>1,143,381</b>	<b>7,248,381</b>	<b>6,105,000</b>	<b>(172,804)</b>	<b>7,075,577</b>
<b>Total Expenses</b>	<b>6,219,079</b>	<b>7,164,674</b>	<b>(1,258,149)</b>	<b>7,481,196</b>	<b>(113,732)</b>	<b>7,367,464</b>	<b>7,481,196</b>	<b>(52,572)</b>	<b>7,428,624</b>

**Kansas Racing and Gaming Commission**  
 Budget Worksheet - Expenditures  
 FY 2020 - FY 2022

**2535 - Expanded Lottery Act Regulation (Gaming) Fund**

		A	B	C	D	E	F	G	I	J
		FY 2020 Actual	FY 2020 Budget	Difference	FY 2021 Approved Budget	Revisions to FY 2021	Revised FY 2021 Budget	FY 2021 Base Budget	Changes from Revised FY 2021 to FY 2022	Submitted FY 2022 Budget
Salaries	510	5,265,915	6,251,083	(985,168)	6,584,263	(119,717)	6,464,546	6,584,263	(55,338)	6,528,925
Shrinkage	519	-	(312,554)	33,025	(329,212)	5,985	(323,227)	(329,212)	2,766	(326,446)
<b>Contractual Services</b>										
Communication	520	64,043	85,200	(21,157)	85,200	-	85,200	85,200	-	85,200
Freight & express	521	3,488	1,300	2,188	1,300	-	1,300	1,300	-	1,300
Printing & advertising	522	842	1,450	(608)	1,450	-	1,450	1,450	-	1,450
Rents	523	223,994	240,650	(16,656)	240,650	-	240,650	240,650	-	240,650
Repairing & servicing	524	109,664	55,708	53,956	55,708	-	55,708	55,708	-	55,708
Travel & subsistence	525	78,085	151,634	(73,549)	151,634	-	151,634	151,634	-	151,634
Fees-other services	526	247,461	316,940	(69,479)	316,940	-	316,940	316,940	-	316,940
Fees-professional services	527	69,247	82,050	(12,803)	82,050	-	82,050	82,050	-	82,050
Other contractual services	529	3,026	19,043	(16,017)	19,043	-	19,043	19,043	-	19,043
<b>Total contractual services</b>		<b>799,850</b>	<b>953,975</b>	<b>(154,125)</b>	<b>953,975</b>	<b>-</b>	<b>953,975</b>	<b>953,975</b>	<b>-</b>	<b>953,975</b>
<b>Commodities</b>										
Clothing	530	9,087	-	9,087	-	-	-	-	-	-
Food	532	-	-	-	-	-	-	-	-	-
Maintenance materials	534	515	4,100	(3,585)	4,100	-	4,100	4,100	-	4,100
Vehicle parts, supplies	535	5,531	28,055	(22,524)	28,055	-	28,055	28,055	-	28,055
Prof. & scientific supplies	536	10,586	25,860	(15,274)	25,860	-	25,860	25,860	-	25,860
Office supplies	537	13,828	74,555	(60,727)	74,555	-	74,555	74,555	-	74,555
Other supplies & materials	539	10,161	4,300	5,861	4,300	-	4,300	4,300	-	4,300
<b>Total commodities</b>		<b>49,708</b>	<b>136,870</b>	<b>(87,162)</b>	<b>136,870</b>	<b>-</b>	<b>136,870</b>	<b>136,870</b>	<b>-</b>	<b>136,870</b>
Capital outlay	54	103,606	135,300	(31,694)	135,300	-	135,300	135,300	-	135,300
<b>Other</b>										
Voluntary Retirement		-	-	-	-	-	-	-	-	-
Interest		-	-	-	-	-	-	-	-	-
Principal		-	-	-	-	-	-	-	-	-
Subtotal		-	-	-	-	-	-	-	-	-
<b>Total Expenditures</b>		<b>6,219,079</b>	<b>7,164,674</b>	<b>(1,225,124)</b>	<b>7,481,196</b>	<b>(119,717)</b>	<b>7,367,464</b>	<b>7,481,196</b>	<b>(55,338)</b>	<b>7,428,624</b>

**Kansas Racing and Gaming Commission**  
 Budget Worksheet - Receipts  
 FY 2020 - FY 2022

**2682 - Gaming Background Investigations Fund**

	A	B	C	D	E	F	G	I	J
	FY 2020 Actual	FY 2020 Budget	Difference	FY 2021 Approved Budget	Revisions to FY 2021	Revised FY 2021 Budget	FY 2021 Base Budget	Changes from Revised FY 2021 to FY 2022	Submitted FY 2022 Budget
Receipts									
Vendor Background Deposits	130,155	300,000	(169,845)	250,000	-	250,000	250,000	(25,000)	275,000
Miscellaneous revenues	-	-	-	-	-	-	-	-	-
State General Fund	-	-	-	-	-	-	-	-	-
Transfer Out	-	-	-	-	-	-	-	-	-
<b>Total Receipts</b>	<b>130,155</b>	<b>300,000</b>	<b>(169,845)</b>	<b>250,000</b>	<b>-</b>	<b>250,000</b>	<b>250,000</b>	<b>(25,000)</b>	<b>275,000</b>
<b>Total Expenses</b>	<b>185,313</b>	<b>333,553</b>	<b>(148,240)</b>	<b>320,227</b>	<b>13,099</b>	<b>332,671</b>	<b>320,227</b>	<b>15,432</b>	<b>335,659</b>

**Kansas Racing and Gaming Commission**  
 Budget Worksheet - Expenditures  
 FY 2020 - FY 2022

**2682 - Gaming Background Investigations Fund**

		A	B	C	D	E	F	G	I	J
		FY 2020 Actual	FY 2020 Budget	Difference	FY 2021 Approved Budget	Revisions to FY 2021	Revised FY 2021 Budget	FY 2021 Base Budget	Changes from Revised FY 2021 to FY 2022	Submitted FY 2022 Budget
Salaries	51	179,013	296,549	(117,536)	298,186	13,099	311,285	298,186	16,244	314,430
Shrinkage	519		(14,827)		(14,909)	(15,564)	(15,564)	(14,909)	(813)	(15,722)
<b>Contractual Services</b>										
Communication	520	-	-	-	-	-	-	-	-	-
Freight & express	521	-	-	-	-	-	-	-	-	-
Printing & advertising	522	-	-	-	-	-	-	-	-	-
Rents	523	-	-	-	-	-	-	-	-	-
Repairing & servicing	524	-	-	-	-	-	-	-	-	-
Travel & subsistence	525	6,019	35,250	(29,231)	35,250	-	35,250	35,250	-	35,250
Fees-other services	526	142	-	142	-	-	-	-	-	-
Fees-professional services	527	-	-	-	-	-	-	-	-	-
Other contractual services	529	-	-	-	-	-	-	-	-	-
<b>Total contractual services</b>		<b>6,161</b>	<b>35,250</b>	<b>(29,089)</b>	<b>35,250</b>	<b>-</b>	<b>35,250</b>	<b>35,250</b>	<b>-</b>	<b>35,250</b>
<b>Commodities</b>										
Clothing	530	-	-	-	-	-	-	-	-	-
Food	532	-	-	-	-	-	-	-	-	-
Maintenance materials	534	-	-	-	-	-	-	-	-	-
Vehicle parts, supplies	535	139	1,700	(1,561)	1,700	-	1,700	1,700	-	1,700
Prof. & scientific supplies	536	-	-	-	-	-	-	-	-	-
Office supplies	537	-	-	-	-	-	-	-	-	-
Other supplies & materials	539	-	-	-	-	-	-	-	-	-
<b>Total commodities</b>		<b>139</b>	<b>1,700</b>	<b>(1,561)</b>	<b>1,700</b>	<b>-</b>	<b>1,700</b>	<b>1,700</b>	<b>-</b>	<b>1,700</b>
Capital outlay	54	-	54	(54)	-	-	-	-	-	-
<b>Total Expenditures</b>		<b>185,313</b>	<b>333,553</b>	<b>(148,240)</b>	<b>320,227</b>	<b>13,099</b>	<b>332,671</b>	<b>320,227</b>	<b>15,432</b>	<b>335,659</b>

**Kansas Racing and Gaming Commission**  
 Budget Worksheet - Receipts  
 FY 2020 - FY 2022

**2734- Illegal Gaming Enforcement Fund**

	A	B	C	D	E	F	G	I	J
	FY 2020 Actual	FY 2020 Budget	Difference	FY 2021 Approved Budget	Revisions to FY 2021	Revised FY 2021 Budget	FY 2021 Base Budget	Changes from Revised FY 2021 to FY 2022	Submitted FY 2022 Budget
Receipts									
Transfer from ELARF									
Seized Assets	-	5,000	(5,000)	5,000	-	5,000	5,000	-	5,000
Miscellaneous Revenues	-	-	-	-	-	-	-	-	-
Fines	113,908	-	113,908	-	-	-	-	-	-
State General Fund	-	-	-	-	-	-	-	-	-
Transfer Out	-	-	-	-	-	-	-	-	-
<b>Total Receipts</b>	<b>113,908</b>	<b>5,000</b>	<b>108,908</b>	<b>5,000</b>	<b>-</b>	<b>5,000</b>	<b>5,000</b>	<b>-</b>	<b>5,000</b>

**Kansas Racing and Gaming Commission**  
 Budget Worksheet - Expenditures  
 FY 2020 - FY 2022

**2734- Illegal Gaming Enforcement Program**

		A	B	C	D	E	F	G	I	J
		FY 2020 Actual	FY 2020 Budget	Difference	FY 2021 Approved Budget	Revisions to FY 2021	Revised FY 2021 Budget	FY 2021 Base Budget	Changes from Revised FY 2021 to FY 2022	Submitted FY 2022 Budget
Salaries	51	-	-	-	-	-	-	-	-	-
Shrinkage	519	-	-	-	-	-	-	-	-	-
<b>Contractual Services</b>										
Communication	520	-	-	-	-	-	-	-	-	-
Freight & express	521	-	-	-	-	-	-	-	-	-
Printing & advertising	522	-	-	-	-	-	-	-	-	-
Rents	523	780	-	780	-	-	-	-	-	-
Repairing & servicing	524	-	-	-	-	-	-	-	-	-
Travel & subsistence	525	70	-	70	-	-	-	-	-	-
Fees-other services	526	-	-	-	-	-	-	-	-	-
Fees-professional services	527	-	-	-	-	-	-	-	-	-
Other contractual services	529	116	3,000	(2,884)	3,000	-	3,000	3,000	-	3,000
Petty Cash Fund Advance		-	-	-	-	-	-	-	-	-
<b>Total contractual services</b>		<b>966</b>	<b>3,000</b>	<b>(2,034)</b>	<b>3,000</b>	<b>-</b>	<b>3,000</b>	<b>3,000</b>	<b>-</b>	<b>3,000</b>
<b>Commodities</b>										
Clothing	530	-	-	-	-	-	-	-	-	-
Food	532	-	-	-	-	-	-	-	-	-
Maintenance materials	534	238	-	238	-	-	-	-	-	-
Vehicle parts, supplies	535	-	1,200	(1,200)	1,200	-	1,200	1,200	-	1,200
Prof. & scientific supplies	536	-	-	-	-	-	-	-	-	-
Office supplies	537	240	-	240	-	-	-	-	-	-
Other supplies & materials	539	-	-	-	-	-	-	-	-	-
<b>Total commodities</b>		<b>478</b>	<b>1,200</b>	<b>(722)</b>	<b>1,200</b>	<b>-</b>	<b>1,200</b>	<b>1,200</b>	<b>-</b>	<b>1,200</b>
Capital outlay	54	2,405	-	2,405	-	-	-	-	-	-
<b>Total Expenditures</b>		<b>3,849</b>	<b>4,200</b>	<b>(351)</b>	<b>4,200</b>	<b>-</b>	<b>4,200</b>	<b>4,200</b>	<b>-</b>	<b>4,200</b>

**Kansas Racing and Gaming Commission**  
 Budget Worksheet - Receipts  
 FY 2020 - FY 2022

**5131 - State Racing Fund**

	A	B	C	D	E	F	G	I	J
	FY 2020 Actual	FY 2020 Budget	Difference	FY 2021 Approved Budget	Revisions to FY 2021	Revised FY 2021 Budget	FY 2021 Base Budget	Changes from Revised FY 2021 to FY 2022	Submitted FY 2022 Budget
Receipts									
Parimutuel tax - live	-	-	-	-	-	-	-	-	-
Parimutuel tax - simulcast	-	-	-	-	-	-	-	-	-
Admissions tax	-	-	-	-	-	-	-	-	-
Fees (License, Registration, etc)	-	1,000	(1,000)	1,000	-	1,000	1,000	-	1,000
Fines	1,723	-	1,723	-	-	-	-	-	-
Unclaimed winnings	-	-	-	-	-	-	-	-	-
Miscellaneous receipts	-	-	-	-	-	-	-	-	-
Operating Transfer out	-	-	-	-	-	-	-	-	-
Transfer In (Racing Funds)	-	-	-	-	-	-	-	-	-
<b>Total Receipts</b>	<b>1,723</b>	<b>1,000</b>	<b>723</b>	<b>1,000</b>	<b>-</b>	<b>1,000</b>	<b>1,000</b>	<b>-</b>	<b>1,000</b>

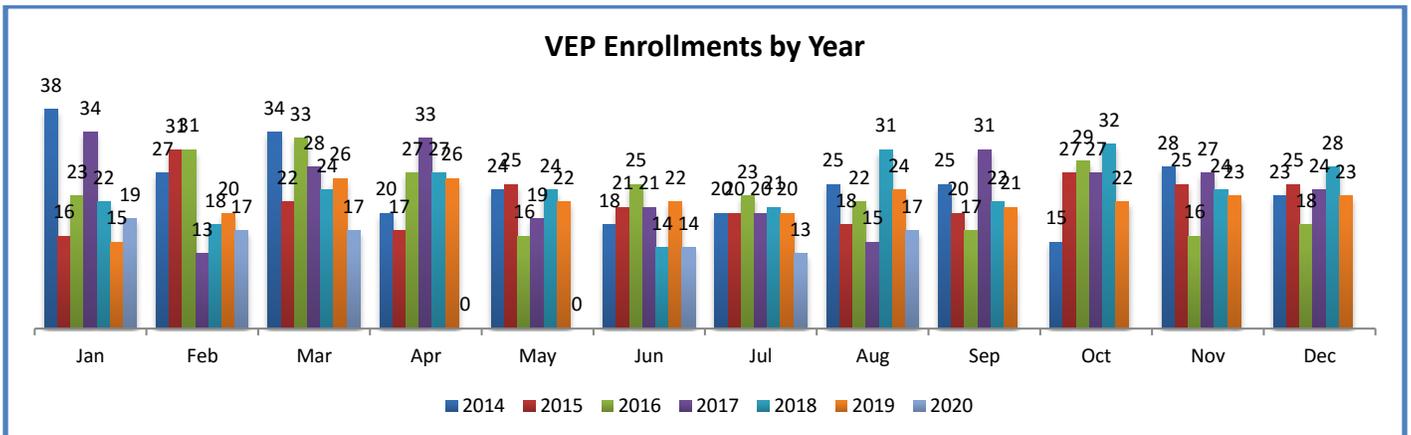
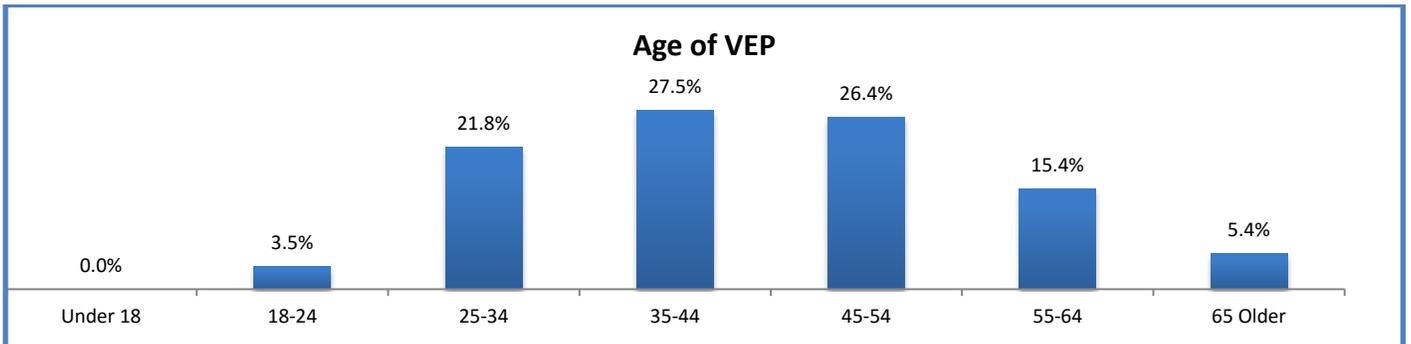
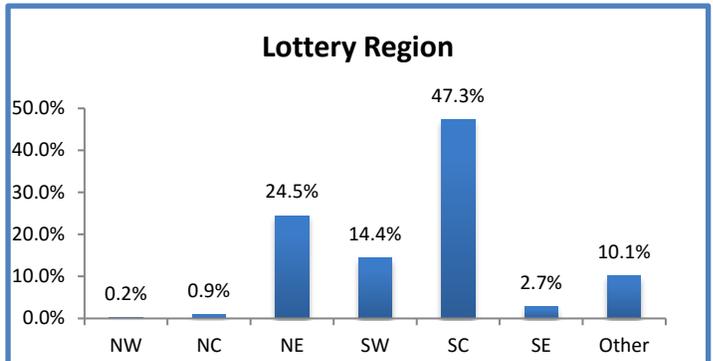
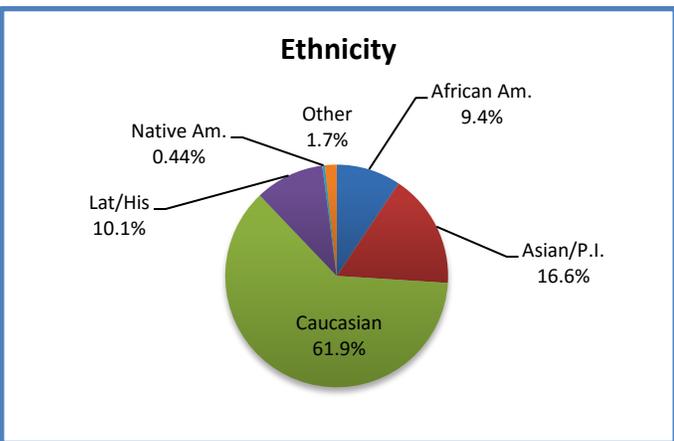
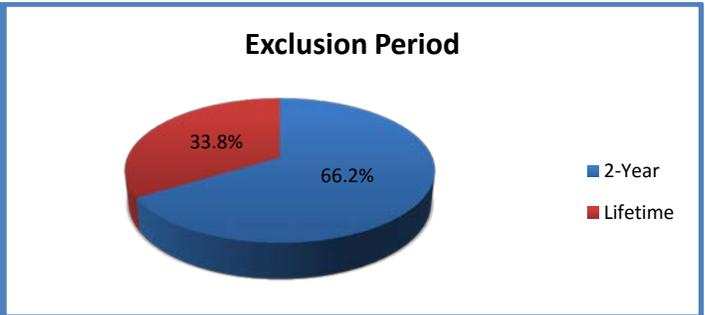
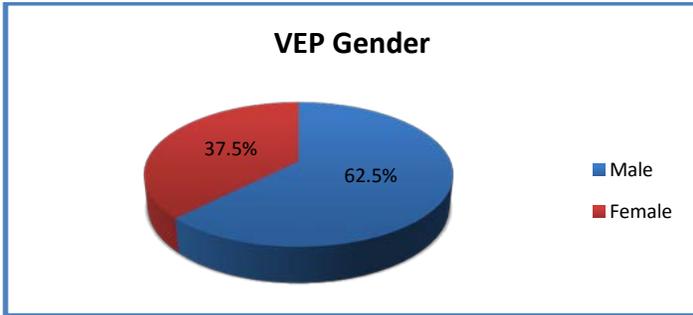
**Kansas Racing and Gaming Commission**  
 Budget Worksheet - Expenditures  
 FY 2020 - FY 2022

**5131 - State Racing Fund**

	A	B	C	D	E	F	G	I	J	
	FY 2020 Actual	FY 2020 Budget	Difference	FY 2021 Approved Budget	Revisions to FY 2021	Revised FY 2021 Budget	FY 2021 Base Budget	Changes from Revised FY 2021 to FY 2022	Submitted FY 2022 Budget	
Salaries	510	1,388	6,369	(4,981)	6,412	(3,227)	3,185	6,412	(3,191)	3,221
Shrinkage	519	-	(318)	-	(312)	153	(159)	(312)	151	(161)
Contractual Services										
Communication	520	-	-	-	-	-	-	-	-	-
Freight & express	521	-	-	-	-	-	-	-	-	-
Printing & advertising	522	-	-	-	-	-	-	-	-	-
Rents	523	-	500	(500)	500	-	500	500	-	500
Repairing & servicing	524	-	-	-	-	-	-	-	-	-
Travel & subsistence	525	-	-	-	-	-	-	-	-	-
Fees-other services	526	-	-	-	-	-	-	-	-	-
Fees-professional services	527	-	500	(500)	500	-	500	500	-	500
Other contractual services	529	-	-	-	-	-	-	-	-	-
Total contractual services		-	1,000	(1,000)	1,000	-	1,000	1,000	-	1,000
Commodities										
Clothing	530	-	-	-	-	-	-	-	-	-
Food	531	-	-	-	-	-	-	-	-	-
Maintenance materials	534	-	-	-	-	-	-	-	-	-
Vehicle parts, supplies	535	-	-	-	-	-	-	-	-	-
Prof. & scientific supplies	536	-	-	-	-	-	-	-	-	-
Office supplies	537	-	-	-	-	-	-	-	-	-
Other supplies & materials	539	-	-	-	-	-	-	-	-	-
Total commodities		-	-	-	-	-	-	-	-	-
Capital outlay	54	-	-	-	-	-	-	-	-	-
Settlement	55	-	-	-	-	-	-	-	-	-
Total Expenditures		1,388	7,051	(5,981)	7,100	(3,074)	4,026	7,100	(3,040)	4,060

## Voluntary Exclusion Program January 2010 – August 2020

Voluntary Exclusions = 2425  
Violation Incidents = 319 (276 individuals)





All Departments		Cash Fund Balances as of August 31, 2020															
DeptID	All	ELARF				Backgrounds				Illegal Gambling				Racing			
All Funds		Beg. Balance	2,362,003			Beg. Balance	177,334			Beg. Balance	127,051			Beg. Balance	69,885		
		Revenue	1,701,523			Revenue	93,254			Revenue	-			Revenue	1,075		
		Expenses	964,687			Expenses	34,450			Expenses	17			Expenses	717		
		End Balance	3,098,839			End Balance	236,138			End Balance	127,034			End Balance	70,243		
Fund	BudgetUnit	Grand Total															
		All Funding Sources															
		YTD FY2020	YTD FY2021	\$ VARIANCE	% VARIANCE	August FY2020	August FY2021	\$ VARIANCE	% VARIANCE	YTD FY2021	YTD FY2021	\$ VARIANCE	% VARIANCE				
		ACTUALS	ACTUALS			ACTUALS	ACTUALS			BUDGET	ACTUALS						
51000	Payroll	847,108	840,586	-6,521	-1%	415,450	406,300	-9,150	-2%	1,060,303	840,586	-219,717	-21%				
10	Shrinkage	0	0	0	0%	0	0	0	0%	-26,507	0	26,507	-100%				
<b>Net Salaries and Wages</b>		<b>847,108</b>	<b>840,586</b>	<b>-6,521</b>	<b>-1%</b>	<b>415,450</b>	<b>406,300</b>	<b>-9,150</b>	<b>-2%</b>	<b>1,033,796</b>	<b>840,586</b>	<b>-193,210</b>	<b>-19%</b>				
52000	Communication	6,889	9,734	2,846	41%	3,856	4,443	587	15%	14,200	9,734	-4,466	-31%				
52100	Freight and Express	804	231	-573	-71%	705	155	-550	-78%	217	231	14	7%				
52200	Printing and Advertising	0	0	0	0%	0	0	0	0%	242	0	-242	-100%				
52300	Rents	52,052	53,347	1,295	2%	90	0	-90	-100%	40,358	53,347	12,989	32%				
52400	Repair/Servicing/Mainten	15	0	-15	-100%	6	0	-6	-100%	9,285	0	-9,285	-100%				
52510	InState Travel and Subsistence	4,611	1,453	-3,158	-68%	2,319	1,298	-1,022	-44%	15,391	1,453	-13,937	-91%				
52520	Out of State Travel and Subsistence	7,266	647	-6,619	-91%	5,144	647	-4,496	-87%	9,882	647	-9,235	-93%				
52530	International Travel and Subsistence	0	0	0	0%	0	0	0	0%	0	0	0	0%				
52600	Fees-Other Services	81,355	70,749	-10,606	-13%	66,495	21,198	-45,296	-68%	52,198	70,749	18,551	36%				
52700	Fee-Professional Services	421	80	-341	-81%	300	80	-220	-73%	20,675	80	-20,595	-100%				
52900	Other Contractual Services	2,447	3,165	718	29%	17	0	-17	-100%	3,091	3,165	74	2%				
<b>Subtotal Contractual Services</b>		<b>155,860</b>	<b>139,407</b>	<b>-16,453</b>	<b>-11%</b>	<b>78,931</b>	<b>27,821</b>	<b>-51,110</b>	<b>-65%</b>	<b>165,538</b>	<b>139,407</b>	<b>-26,131</b>	<b>-16%</b>				
53200	Food for Human Consumption	0	0	0	0%	0	0	0	0%	17	0	-17	-100%				
53400	Maint Constr Material Supply	50	30	-20	-40%	50	30	-20	-40%	567	30	-537	-95%				
53500	Vehicle Part Supply Accessory	1,172	685	-487	-42%	658	285	-373	-57%	4,776	685	-4,090	-86%				
53600	Pro Science Supply Material	17	-799	-816	-4702%	17	-799	-816	-4702%	4,793	-799	-5,592	-117%				
53700	Office and Data Supplies	642	1,346	705	110%	316	1,346	1,031	327%	12,426	1,346	-11,080	-89%				
53900	Other Supplies and Materials	1,556	3,207	1,651	106%	1,272	3,143	1,871	147%	717	3,207	2,490	347%				
<b>Subtotal Commodities</b>		<b>3,437</b>	<b>4,469</b>	<b>1,032</b>	<b>30%</b>	<b>2,313</b>	<b>4,005</b>	<b>1,692</b>	<b>73%</b>	<b>23,295</b>	<b>4,469</b>	<b>-18,826</b>	<b>-81%</b>				
54000	<b>TOTAL Capital Outlay</b>	<b>19,799</b>	<b>15,408</b>	<b>-4,391</b>	<b>-22%</b>	<b>16,046</b>	<b>15,408</b>	<b>-637</b>	<b>-4%</b>	<b>22,550</b>	<b>15,408</b>	<b>-7,142</b>	<b>-32%</b>				
55960	Vol Retirement Incentive	0	0	0	0%	0	0	0	0%	0	0	0	0%				
56000	Debt Service - Principal	0	0	0	0%	0	0	0	0%	0	0	0	0%				
56100	Payments for Interest and Service	0	0	0	0%	0	0	0	0%	0	0	0	0%				
<b>Subtotal VRIP and Debt Service</b>		<b>0</b>	<b>0</b>	<b>0</b>	<b>0%</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0%</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0%</b>				
<b>Grand Total</b>		<b>1,026,204</b>	<b>999,871</b>	<b>-26,334</b>	<b>-3%</b>	<b>512,739</b>	<b>453,534</b>	<b>-59,205</b>	<b>-12%</b>	<b>1,245,178</b>	<b>999,871</b>	<b>-245,308</b>	<b>-20%</b>				

\*This report has not been audited by the State of Kansas and is intended solely for the use of the Executive Director of the Kansas Racing and Gaming Commission.

# September 2020 - August 2021

## Kansas Racing and Gaming Commission Planner

Sep 2020						
S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

### SEPTEMBER

*11 Commission Meeting*

### OCTOBER

*16 Commission Meeting*

### NOVEMBER

*13 Commission Meeting*

### DECEMBER

*11 Commission Meeting*

### JANUARY

*15 Commission Meeting*

### FEBRUARY

*12 Commission Meeting*

### MARCH

*12 Commission Meeting*

### APRIL

*16 Commission Meeting*

### MAY

*14 Commission Meeting*

### JUNE

*11 Commission Meeting*

### JULY

*16 Commission Meeting*

### AUGUST

*13 Commission Meeting*

Mar 2021						
S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Oct 2020						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Apr 2021						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Nov 2020						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

May 2021						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Dec 2020						
S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Jun 2021						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Jan 2021						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Jul 2021						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Feb 2021						
S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28					

Aug 2021						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						