STANDARD SERIES

GLI-20:

Kiosks

Version: 1.4

Release Date: July 1, 2006

This Page Intentionally Left Blank

ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International, Inc. (GLI)** for the purpose of providing independent certifications to suppliers under this Standard and complies with the requirements set forth herein.

A supplier should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, Gaming Laboratories International, Inc. will provide a certificate of compliance along with an appropriate *Gaming Labs Certified*™ mark evidencing the certification to this Standard.

Kiosks

GLI-20 Revision 1.4

Date Released: July 1, 2004 (V1.4)
Date Released: May 3, 2004 (V1.3)
Date Released: February 20, 2003 (V1.2)
Date Released: January 31, 2003 (V1.1)
Date Released: December 4, 2002 (V1.0)
Date Created: December 4, 2002

REVISION HISTORY

REV 1.4

- Modifications made throughout the document to permit the function of receiving a redeemable ticket, at the kiosk. In addition, supporting equipment (i.e., hoppers, printers) technical specifications were added to accommodate this functionality.
- Document title was changed from "Redemption Terminals" to "Kiosks" as there are further features addressed that do not only pertain to "Redemption".

REV 1.3

Formatting changes only

REV 1.2

1.2.1 changed the reference from 'paid' to 'redeemed'.
2.4.1(d) & (e) added '*' then added a note indicating that these requirements only apply to programs stored on EPROM since the type, size and position would only apply to EPROM.
3.1.2 modified the requirement for the terminal ID where it is now not required to be on the 'exterior' of the cabinet. The rule now does not dictate where the ID is to be located, however, the ID itself is still required.
3.1.6 was changed to eliminate the Note Acceptor Stacker requirements that required a separate key to access the stacker and another key to remove the bills. This change was made since the level of security should be mandated by the local gaming commission and is not a technical requirement.
3.2.3 was modified to include information on critical memory for devices that use hard drive for the program storage media.
3.3.1 was modified to indicate the network security must be implemented by the casino's IT department since the kiosk has no control over how each casino implements network security.
4.1.1 was modified to remove the reference to a 'secure' protocol. See mod to 3.3.1, above.
4.2.1(b) has been changed to remove the requirement for the error conditions 'system link down' and 'communication timed out' and reworded (b) to more clearly state 'system and kiosk not communicating (this may be detected upon ticket insertion only)'. (c) & (d) are now reserved since combined with (b).

REV 1.1

1.2.1 changed the reference from 'paid' to 'redeemed'.
3.1.1 clarified that the main door is to be locked.
3.2.2(b) excluded kiosks that use printers to store the log information.
4.1.1 was clarified to use a secure communication protocol when communicating with the system.

4.1.2 Communication Protocol section was removed and is now referenced within 4.1.1. The requirements throughout this section would limit the method of communication. Therefore, it was removed and the change to 4.1.1 would allow for any method of communication provided the method is secure.

4.2.1 reformatted to incorporate all error conditions into this section.

4.3 removed this section. It is now RESERVED. Everything was incorporated within 4.2.1.

4.3.2 was changed to no longer require a maximum ticket amount of $3,000.00 since this will be jurisdiction. specific. The rule now allows for a fixed amount or a selectable amount. If the manufacturer uses a fixed amount, it may be necessary for the manufacturer to produce jurisdiction specific software.

4.6.1 changed to allow for a printer to be used to store the required logs however the device must be capable of detecting printer disconnection, printer jam and paper out conditions.

4.8.1 was changed to clarify the authentication 'must' be accomplished (previously indicated 'can') be authenticated by a third-party device. This section was also changed to allow for the program manufacturer to embed the verification program within the device code, provided the manufacturer receives written approval before submitting the program to the test laboratory for testing. Also, required a means to extract the program from the device must be submitted to the laboratory.

Table of Contents

CHAPTER 1

1.0 OVERVIEW – Kiosks

1.1. Introduction

1.1.1 ***Kiosks Defined***.   Kiosks are player interface units that may be used to perform various tasks including, but not limited to:

a) <u>Voucher/Coupon Redemption</u> - Kiosks are usually interfaced to some type of monitoring or control system that will play a role in the critical functions of the kiosk. Gaming Devices that have the option of issuing payments via ticket voucher printers must be interfaced to a Validation System as explained in GLI-11 and in GLI-13.   When a ticket voucher is redeemed for cash, the ticket voucher on the Validation System must be updated to reflect a 'Redeemed' status.   When using a Kiosk as the method of redemption, the Kiosk shall read the ticket voucher and notify the Validation System of all required validation information. The system is then to determine if the ticket voucher is valid and transmit to the Kiosk the amount to be paid or instruct the kiosk to reject the ticket voucher. For valid vouchers, payment is made to the patrons from various denominations' coin and currency payment mechanisms.

b) <u>Bill Breaking</u> – Bill Breaking is the act of making change. A patron may wish to insert a bill for any combination of change. It may include an insertion of a large denomination bill for the issuance of smaller denomination bills. It may also include the insertion of small denomination bills for the issuance of coin.

c) <u>Ticket Issuance</u> - Ticket issuance kiosks that issue tickets/vouchers via ticket voucher printers, must be interfaced to a validation system. When a ticket/voucher is printed from the kiosk the ticket/voucher on the validation system must be updated to reflect a 'Pending' status. The ticket issuance kiosk must receive all its validation information

from the ticket validation system. The ticket validation system must ensure that the correct information is sent to the ticket issuance kiosk and the kiosk must validate the incoming message packets through an error checking mechanism before printing a ticket. When the ticket voucher printed by the kiosk is redeemed at a gaming device, cashiers cage or kiosk, the system must change the 'Pending' status of the ticket voucher to 'Redeemed'.

d) <u>Promotional Point Redemption</u> - Promotional Point Redemption defines the process of a patron redeeming their promotional player points at the kiosk for cash or a ticket/voucher. The kiosk in this case is being used as an alternative to the current process of the player approaching the casino cage or player services desk to redeem their points. The kiosk in this case shall only be interfaced to an approved promotional system/gateway. This standard will only address the use of kiosks when redeeming player points for cash or ticket/voucher. This standard will not address the use of kiosks for redemption of player points for casino merchandise and/or services.

e) <u>Information Reporting</u> – The kiosk can be used to display marketing information for customers. This feature is not covered by this standard as it does not affect the integrity of gaming.

1.1.2 ***<u>Phases of Certification</u>***. The certification of a Kiosk shall be based on laboratory testing, where the laboratory will test the integrity of the kiosk in conjunction with each compatible system(s) along with compliance with this document.

1.2   Purpose of Standard

1.2.1 ***<u>General Statement</u>***.   The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Kiosk operations;

b) To only test those criteria which impact the credibility and integrity of gaming from both the revenue collection and security point of view;

c) To create a standard that will ensure that Kiosks in Casinos are fair, secure, and able to be audited and operated correctly;

d) To distinguish between local public policy and laboratory criteria. At GLI, we believe that it is up to each local jurisdiction to set their public policy with respect to gaming;

e) To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this standard but left to appropriate test laboratories that specialize in that type of testing. Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment;

f) To construct a standard that can be easily changed or modified to allow for new technology; and

g) To construct a standard that does not specify any particular technology, method or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time, to encourage new methods to be developed.

1.2.2   *No Limitation of Technology*.   One should be cautioned that this document should not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this standard, make changes and incorporate new minimum standards for the new technology.

1.2.3   *Scope of Standard*. This standard will only provide technical requirements for Kiosk features, which would affect player fairness, revenue accounting, and security.

1.3   Other Documents That May Apply

1.3.1   *General Statement*. This standard covers the minimal requirements for Kiosks. The following other standards may apply:

a) Gaming Devices in Casinos (GLI-11);

b) On-line Monitoring and Control System (MCS) and Validation Systems in Casinos (GLI 13); and

c) Cashless Systems in Casinos (GLI-16)

d) Individual Gaming Board Minimum Internal Control Procedures.

CHAPTER 2

2.0 SUBMISSION REQUIREMENTS

2.1 Introduction

2.1.1 ***General Statement***. This chapter shall govern the types of information that are, or may be required to be submitted by the submitting party in order to have equipment tested to this Standard. Where the information has not been submitted or is not otherwise in the possession of the test laboratory, the submitting party shall be asked to supply additional information. Failure to supply the information can result in denial in whole or in part of the submission and/or lead to testing delays.

2.2 Kiosk Submissions

2.2.1 ***General Statement***. A Prototype (full submission) submission is a first time submission of a particular piece of hardware or software that has not previously been reviewed by the test laboratory.   For Modifications of previous submissions, whether certified or pending certification, see 'Modifications to a Prototype Submission,' Section 2.2.6.

NOTE: Due to abnormal component complexity and/or excessive cost it is sometimes necessary for on-site testing of a system at the manufacturer's facility. Regular upgrades normally preclude testing at the manufacturer's facility except in the case of prototype submissions.

2.2.2 ***Presentation of Equipment to the Test Laboratory; Identical Equipment***.   Each item of gaming equipment supplied by a manufacturer to the field shall be functionally identical to the specimen tested and certified. For example, an interface element supplied as a certified device shall not have different internal wiring, components, firmware, circuit boards, circuit board track cuts or circuit board patch wires from the certified specimen, unless that change is also certified.

2.2.3 ***Submission Letter Requirements***. Each submission shall include a request letter, on company letterhead, dated within one (1) week of the date the submission is received by the test laboratory. The letter should include the following:

a) The jurisdiction(s) for which you are requesting certification;

b) The items requested for certification. In the case of software, the submitting party shall include ID numbers and revision levels, if applicable. In the case of proprietary hardware, the submitting party shall indicate the manufacturer, model, and part and revision numbers of the associated components of hardware; and

c) A contact person who will serve as the main point of contact for engineering questions raised during evaluation of the submission. This may be either the person who signed the letter or another specified contact.

2.2.4 ***Inventory of Equipment to the Test Laboratory***. Each ticket voucher Kiosk submission must include all components needed to configure the Kiosk with the system(s) it's compatible with, as it would be configured in a live casino environment. This includes all communication, bill acceptor, printer, etc. hardware and software.

2.2.5 ***Accompanying Documentation/Components***. The following items shall accompany each Kiosk submission:

a) If applicable, all UL, CSA, EC, AS3100, etc. or equivalent certification, see also Sections 3.1.3 and 3.1.4. This certification information may be supplied at a later date;

b) Any other proprietary equipment that may be used in the field in conjunction with the Submission, if necessary to test the requirements set forth, unless the laboratory already possesses;

c) Two sets of all EPROMs, CD-ROMs, or other storage media (if other storage media, the items described within section 4.8.1(NOTE) may be required as well) which contain identical contents. This includes all program executables, system component firmware,

bin files, etc. Where the test laboratory already has tested a software component, resubmission may not be necessary;

d) Documentation pertaining to all available options and instructions on configuring each option;

e) Documentation describing how to add the Kiosk to the Validation System. Include any specific flags or fields used to identify the Kiosk separately from gaming devices. (e.g., "Kiosk is entered as a gaming device with a number greater than 9999" or "Kiosk is entered as a slot machine with flag called 'calculation type' set to Other," etc.);

f) Source Code, a Link Map and Symbol Table for all primary software executables. In addition, if requested, explanation of all non-volatile RAM on any system device with the non-volatile RAM locations described;

g) All user manuals in both hard and soft copy format to include a general overview of the system from a component level, software and hardware setup and integration, and system block diagrams and flow charts for the communication program, if required;

h) If not included in the user manuals, a connectivity manual for all unique Validation Systems capable of being interfaced if applicable; wiring diagrams depicting connection points to devices, power, etc.; and identification by part number or some other scheme, any unique wiring harnesses, and ancillary boards required for communication of a particular device;

i) If not included in the user manuals, a list of all supported communication protocols specifying version, if applicable;

j) If utilizing a software verification algorithm provide a description of the algorithm, theoretical basis of the algorithm, results of any analyses or tests to demonstrate that the algorithm is suitable or the intended application, rules for selection of algorithm coefficients or "seeds", and means of setting the algorithm coefficients or "seeds;" and

k) If completed by the manufacturer, provide a system test plan and results to detail gaming devices and software versions the Kiosk was tested with.

NOTE: Where the testing laboratory has been previously supplied with the information on a previous submission, duplicate documentation is not required, provided that the previous information is referred to by the submitting party, and those documents are easily located at the

testing laboratory. Every effort shall be made to reduce the redundancy of submission information.

2.2.6 **_Modifications to a Prototype Submission_**. Submissions of modifications to the Prototype submission, including hardware changes and/or software changes, shall include, if applicable:

a) The jurisdiction(s) for which you are requesting certification;

b) The items requested for certification. In the case of software, the submitting party shall include ID numbers and revision levels, if applicable. In the case of proprietary hardware, the submitting party shall indicate the manufacturer, model, and part and revision numbers of the associated components of hardware;

c) A list of the system(s) the kiosk will be connected to, including the minimum supported system version number(s). A description of any system application(s) needed to interface to the system(s), including the minimum supported system application version numbers; and

d) A contact person who will serve as the main point of contact for engineering questions raised during evaluation of the submission. This may be either the person who signed the letter or another specified contact.

2.3   Software Programming Requirements and Compilation

2.3.1 **_General Statement_**.   The following items shall be contained within all submitted source code or related modules:

a) Module Name;

b) Brief description of module function; and

c) Edit History, including who modified it, when and why.

2.3.2 <u>**Source Code Commented**</u>.   All source code submitted shall be commented in an informative and useful manner.

2.3.3 <u>**Source Code Completeness**</u>.   All source code submitted shall be correct, complete and able to be compiled.

2.4   Program Identification

2.4.1 <u>**Firmware Requirements**</u>.   On the system firmware submitted and subsequently placed in the field, each program shall be uniquely identified, displaying:

a) Program ID ;

b) Manufacturer;

c) Version number;

d) *Type and size of medium (requirement can be met by manufacturer stamp); and

e) *Location of installation in interface element device, if potentially confusing.

* Applies to EPROM only.

NOTE: For EPROM based firmware, the identification label shall be placed over the UV window to avoid erasing or alteration of the program.

2.5   Joint Venture Submissions

2.5.1 <u>**General Statement**</u>.   A system is considered a joint venture when two or more companies are involved in the manufacturing of one system. Due to the increasing amount of joint venture submissions (more than one supplier involved in a product submission) and to alleviate any confusion to the suppliers, our regulator clients and our firm, GLI has set forth the following procedures for such submissions:

a) One company will prepare and submit the entire submission, even if they are using parts from other suppliers, and must identify all part numbers of all components. This will be the primary contact for the submission;

b) The company submitting an approval request should do so on their letterhead. GLI will delegate an internal file number in this company's name and will bill this company for all costs incurred throughout the approval process;

c) The primary contact will be called when questions arise. However, GLI engineers will work with all parties involved, completing the review;

d) All suppliers who are part of the submission "group" may need to be licensed in the jurisdiction(s) where the submission is being approved. As a courtesy to the supplier, GLI may inquire as to whom does not need to be licensed from the regulator client. It should be noted that licensing questions should be handled directly with the jurisdiction; and

e) Upon completion, it is the primary contact company that will receive the approval letter, provided the submission meets the jurisdictional requirements. The primary contact company may then release copies of the approval letter to the associated manufacturer(s).

CHAPTER 3

3.0 HARDWARE REQUIREMENTS

3.1 Terminal Requirements

3.1.1 **_Cabinet Security_**.   The main door, that must be locked, shall be manufactured of materials that are suitable for allowing only legitimate access to the inside of the cabinet. Doors and their associated hinges shall be capable of withstanding determined illegal efforts to gain access to the inside of the Kiosk, and shall leave evidence of tampering if an illegal entry is made.

 3.1.2 **_Cabinet Wiring_**. The Kiosk shall be designed so that power and data cables into and out of the kiosk can be routed so that they are not accessible to the general public. This is for kiosk integrity reasons only, not for health and safety. Security-related wires and cables that are routed into a logic area shall not be able to be easily removed.

3.1.3 **_On/Off Switch_**. An on/off switch that controls the electrical current shall be located in a place which is readily accessible within the interior of the machine so that power cannot be disconnected from outside of the machine using the on/off switch. The on/off positions of the switch shall be labeled.

3.1.4 **_Switches and Jumpers_**. If the Kiosk contains 'Switches and Jumpers', all switches or jumpers shall be fully documented for evaluation by the test laboratory.

3.1.5 **_Terminal Identification_**. The Kiosk must have an identification badge that is not removable without leaving evidence of tampering affixed to the cabinet that must include the following information:

a) Manufacturer's Name;

b) Unique Serial Number;

c) Kiosk Model Number; and

d) Date of Manufacture.

3.1.6 ***Player Safety***. Electrical and mechanical parts and design principals of the electronic associated hardware may not subject a player to any physical hazards. The test laboratory shall NOT make any finding with regard to Safety and EMC testing as that is the responsibility of the manufacturer of the goods or those that purchase the goods. Such Safety and EMC testing may be required under separate statute, regulation, law or Act and should be researched, accordingly, by those parties who manufacture or purchase said hardware. The test laboratory shall not test for, be liable for, nor make a finding relating to these matters.

3.1.7 ***Kiosk Integrity***. The Laboratory will perform certain tests to determine whether or not outside influences affect performance to the player or create cheating opportunities. A Kiosk shall be able to withstand the following tests, resuming operation without operator intervention:

a) Electro-magnetic Interference. Kiosks shall not create electronic noise that affects the integrity or fairness of the neighboring associated equipment;

b) Electro-static Interference. Protection against static discharges requires that the system's hardware be earthed in such a way that static discharge energy shall not damage or inhibit the normal operation of the electronics or other components within the System. Systems may exhibit temporary disruption when subjected to a significant electro-static discharge greater than human body discharge, but they shall exhibit a capacity to recover and complete any interrupted function without loss or corruption of any control or data information associated with the System. The tests will be conducted with a severity level of up to 27KV air discharge;

NOTE: For commercial components that are affected (e.g. a PC monitor), there must be a method to determine the state the Kiosk was in if any of the components fail from static discharge.

c) Radio Frequency Interference (RFI). Systems shall not divert from normal operation by the application of RFI at a frequency range from 27 to 1000 MHz with a field strength of 3 volts per meter; and

d) Magnetic Interference. Systems shall not be adversely affected by Magnetic Interference. The manufacturer should supply any documentation if the device has had Magnetic Interference testing against any recognized standard.

3.1.8 _Tower Light_. There should be a light on top of the terminal that is clearly visible that automatically illuminates when any of the Error Conditions occur or the 'Call Attendant' (if applicable) is initiated by the patron. This requirement may be substituted for a notification system that alerts casino staff of error conditions.

3.1.9 _External Doors/Compartment Requirements_. The interior of the device should not be accessible when all doors are closed and locked. Doors shall be manufactured of materials that are suitable for allowing only legitimate access to the inside of the cabinet. (ie: doors and their associated hinges shall be capable of withstanding, determined illegal efforts to gain access to the inside of the kiosk and shall leave evidence of tampering if an illegal entry is made).

3.1.10 _The Logic Door and Logic Area_. It is recommended the Kiosk utilize a logic area which is a locked cabinet area (with its own locked door) which houses electronic components* that have the potential to significantly influence the operation of the kiosk, there may be more that one such logic area in a kiosk.

* Electronic component items that are recommended to be housed in one(1) or more logic areas are:

a) CPUs and other electronic components involved in the operation of the kiosk

b) Electronics and components housing display program storage medium (passive display equipment exempted);

c) Communication controller electronics and components housing the communication program storage media or the communication board for the on-line system may reside outside the kiosk and

d) All flash memory devices that affect the kiosk play function of the kiosk.

3.1.11 _Coin and Currency Compartments_. GLI recommends the coin and currency compartments shall be locked separately from the main cabinet area. It is also recommended that the kiosk be fitted with sensors that indicate door open/close or stacker removed.

3.1.12 _Video Monitors/Touch Screens_. Shall meet the following rules:

a) A touch screen (if applicable) shall be accurate and once calibrated shall maintain that accuracy for at least the manufacturer's recommended maintenance period;

b) A touch screen (if applicable) should be able to be re-calibrated by venue staff without access to the machine cabinet other than opening the main door; and

c) There shall be no hidden or undocumented buttons/touch points (if applicable) anywhere on the screen.

3.1.13 _Back-up of Memory_. The Kiosk must utilize battery back up, or an equivalent, that is capable of maintaining the accuracy of all Critical Memory for thirty (30) days after power is discontinued from the Kiosk.

3.2   Coin Acceptors and Diverters

3.2.1 _Diverter_. For kiosks that accept coins or tokens, the software shall ensure that the diverter directs coins to the hopper or to the drop box when the hopper is full. The hopper full detector shall be monitored to determine whether a change in diverter status is required. If the state of the detector changes the diverter shall operate as soon as possible after a state change without causing a disruption of coin flow or creating a coin jam. Hopper-less kiosks shall always divert coins to the drop box.

3.2.2 ***Coin or Token Acceptors***. If the kiosk uses a coin acceptor the acceptor shall accept or reject a coin on the basis of metal composition, mass, composite makeup or equivalent security. In addition, it shall meet the following rules:

a) Coin Acceptor Security Features/Error Conditions: The coin acceptor shall be designed to prevent the use of cheating methods such as slugging (counterfeit coins), stringing (coin pullback), the insertion of foreign objects and other manipulation;

b) Rapidly Fed Coins: The kiosk shall be capable of handling rapidly fed coins or piggy backed coins so that occurrences of cheating are eliminated;

c) Direction Detectors: The kiosks shall have suitable detectors for determining the direction and the speed of coin travel in the receiver. If a coin traveling at too slow of a speed or improper direction is detected the kiosk shall enter an error condition and display an error condition for at least thirty (30) seconds or be cleared by an attendant;

d) Invalid Coins: Coins deemed invalid by the acceptor shall be rejected to the coin tray and shall not be counted as credits;

e) Coin Acceptance Conditions: Acceptance of coins for crediting to the transaction meter shall only be possible when the kiosk is enabled for play. Other states, such as error conditions, including door opens and audit mode shall cause the disabling of the coin acceptor system.

3.3   Bill Acceptors

3.3.1 ***Bill Acceptors***. All acceptance devices shall be able to detect the entry of valid bills, coupons, paper, tokens or other approved notes, if applicable and provide a method to enable the kiosk software to interpret and act appropriately upon a valid or invalid input. The acceptance device(s) shall be electronically-based and be configured to ensure that they only accept bills of legal tender. The bill input system shall be constructed in a manner that protects against vandalism, abuse or fraudulent activity. In addition, credits shall only be registered when:

a) The bill or other note has passed the point where it is accepted and stacked; and

b) The acceptor has sent the "irrevocable stacked" message to the machine.

3.3.2 *Communications*. All bill acceptors shall communicate to the kiosk using a bi-directional protocol.

3.3.3 *Factory Set Bill Acceptors*. If bill acceptors are designed to be factory set only it shall not be possible to access or conduct maintenance or adjustments to those bill acceptors in the field, other than:

a) The selection of bills, coupons, paper, tokens or other approved notes and their limits;

b) Changing of certified EPROMs or downloading of certified software;

c) Adjustment of the tolerance level for accepting bills or notes of varying quality should not be allowed externally to the machine. Adjustments of the tolerance level should only be allowed with adequate levels of security in place. This can be accomplished through lock and key, physical switch settings or other accepted methods approved on a case by case basis;

d) Maintenance, adjustment and repair per approved factory procedures; or

e) Options that set the direction or orientation of acceptance.

3.3.4 *Bill Acceptor Requirements* A bill acceptor shall not be adversely affected by the following:

a) Electro-static discharge;

b) Power surges;

c) Radio frequency interference;

d) Electro-magnetic interference;

e) Environmental extremes;

f) Interconnecting cables from the bill acceptor devices to the kiosk shall not be exposed external to the kiosk; and

g) The manufacturer should supply any documentation if the bill acceptor has had any of the above tests performed by a recognized standard.

3.3.5   *Bill Acceptor Stacker Requirements*. Each bill acceptor shall have a secure stacker and all accepted bills shall be deposited into the secure stacker. The secure stacker is to be attached to the kiosk in such a manner so that it cannot be easily removed by the physical force and shall meet the following rules:

a) The bill acceptor device shall have a 'stacker full' sensor

b) It is recommended there be a separate key to access the stacker area. This key shall be separate from the main door. In addition, a separate key shall be required to remove the bills from the stacker; and

c) A tower light or alarm shall be activated whenever there is access to the bill door or the stacker has been removed.

3.3.6   *Self Test* The bill acceptor device shall perform a self test at each power up. In the event of a self test failure the bill acceptor shall automatically disable itself (i.e: enter bill reject state) until the error state has been cleared.

CHAPTER 4

4.0 SOFTWARE REQUIREMENTS

4.1   Memory Requirements

4.1.1   *Critical Memory*. Critical memory is used to store all data that is considered vital to the continued operation of the Kiosk. This includes, but is not limited to:

a) All Electronic Meters, as defined by this document;

b) Ticket Voucher Redeemed Log, provided the log is not stored on printed paper within the device; and

c) The last normal state the Kiosk software was in before interruption.

4.1.2   *Function of RAM Reset*. Following the initiation of a RAM reset procedure (utilizing a certified RAM Clear method) the program shall execute a routine which initializes each and every bit in RAM to the default state.

4.1.3   *Maintenance of Critical Memory*. Critical memory storage shall be maintained by a methodology that enables errors to be identified and corrected in most circumstances. This methodology may involve signatures, checksums, partial checksums, multiple copies, timestamps and/or effective use of validity codes.

NOTE: If hard drive file storage of critical memory elements is used, the critical data must be maintained accurately. The laboratory will review the method used on a case-by-case basis.

4.1.4   *Data Alteration*. The Kiosk shall not permit the alteration of any Meter or Error Condition log information without supervised access controls. In the event Meter or Error Condition log data is changed, an audit log must be capable of being produced to document:

a) Data element altered;

b) Data element value prior to alteration;

c) Data element value after alteration;

d) Time and Date of alteration; and

e) Personnel that performed alteration (user login).

4.2   Communication

4.2.1   Communication Components.   For Ticket or Coupon Issuance and/or Redemption features, the Kiosk must be designed to allow for communication with a Validation System. All communications between the Kiosks and the Validation System must be secured. This network security must be implemented by the casino's Information Technology (IT) department.

4.3   Error Conditions

4.3.1   General Statement.   The Kiosk must be capable of detecting and displaying the following Error Conditions. The Error Condition must illuminate the tower light or sound an audible alarm. The Kiosk shall be able to recover to the state it was in immediately prior to the interruption occurring, including during payment.   Error Conditions requiring attendant intervention are denoted by '*':

a) Power loss or power reset;

b) System   and Kiosk not communicating (this may be detected upon ticket insertion/issuance request only)

c) Coin or currency out error*;

d) Coin Hopper or Cash Dispenser empty or timed out *(should not require immediate intervention if alternate method of payment available (e.g. 6 dollar ticket and 5 dollar bill hopper out but unit could still pay in ones from the 1 dollar hopper));

e) RAM error (critical memory)*;

f) Low RAM battery (if battery external to the RAM itself used)*;

i)   Ticket voucher-in jam*;

j)   Door open (all external doors);

k)   Bill acceptor stacker full (this condition should cause the Bill Acceptor to disable itself to no longer accept anything);

l)   Bill acceptor door open;

m) Stacker door open or stacker removed; and

n)   Printer* errors, where applicable, which would include:

    1.   Out of paper/paper low;

    2.   Printer jam/failure; and

    3.   Printer disconnected – which may only be detected when the software tries to print.

NOTE: If the Kiosk uses error codes instead of a text explanation of the Error Conditions, a description of error codes and their meanings must be affixed on the inside of the Kiosk.

NOTE: If any of the above Error Conditions occur during the acceptance and/or escrowing of a ticket voucher, the ticket voucher must be returned to the patron without a status change on the Validation System or, once the Error Condition is cleared, proceed to pay the patron and have a status of 'Redeemed' on the system.

4.4   Program Interruption & Resumption

4.4.1   ***Interruption***. When the kiosk's main door is opened, the Kiosk shall cease activity, enter an error condition, display an appropriate error message, disable coin acceptance and bill acceptance, and either sound an alarm or illuminate the tower light or both. Following any program interruption (e.g., power down), the software shall be able to recover to the state it was in immediately prior to the interruption occurring.

4.4.2 ___Resumption___. On program resumption, the kiosk shall return to it's original state and perform the following procedures:

a) Any communications to an external device shall not begin until the program resumption routine, including self-tests, is completed successfully;

b) Kiosk control programs shall test themselves for possible corruption due to failure of the program storage media. The authentication may use the checksum; however, it is preferred that the Cyclic Redundancy Check (CRC) calculations is used as a minimum (at least 16 bit). Other test methodologies shall be of a certified type; and

c) The integrity of all critical memory shall be checked.

4.5 Transaction Limits

4.5.1 ___General Statement___. Each Kiosk must have the ability to have transaction limits for ticket issuance and also ticket redemption, where applicable. The configuration of the transaction limit must be via a secure means. The local Gaming Commission, if required, will determine the transaction limit.

4.6 Metering

4.6.1 ___General Statement___. Electronic metering information is to be maintained in critical memory at the Kiosk and shall be accessible only by an authorized person.

4.6.2 ___Accounting Meters___. Electronic accounting meters shall be at least eight (8) digits in length. If the meter is being used in dollars and cents, at least eight (8) digits must be used for the dollar amount. The meter must roll over to zero upon the next occurrence, any time the meter is eight (8) digits or higher and after 99,999,999 has been reached or any other value that is logical. The following accounting information must be maintained within Critical Memory:

a) A "Total In" Meter(s) that accumulates the total value of all coins, bills, vouchers and coupons accepted by the device. Separate In meters shall report the value of all tickets redeemed and the value of all bills redeemed and the value of all coins redeemed; and

b) A "Total Out" Meter(s) for payments issued by the machine. Separate 'Out Meters' shall report the value of all coins, bills and tickets dispensed by the machine.

c) A "Handpay" meter shall reflect the cumulative amounts paid by an attendant in the event that a ticket cannot be printed

4.6.3 _Occurrence Meters_. Occurrence meters shall be at least three (3) digits in length and roll over to zero upon the next occurrence any time the meter is higher that the maximum number of digits. The following occurrence information must be maintained within Critical Memory:

a) A meter shall accumulate the number of times the external doors are opened;

b) A meter shall accumulate the number of times the cash area doors are opened;

c) Total number of all notes accepted by the Bill Acceptor; and

d) A breakdown of each note type accepted by the Bill Acceptor, bills by denomination.

4.7 Verification

4.7.1 _General Statement_. The device shall have the ability to allow for an independent integrity check of the device's software from an outside source. This must be accomplished by being authenticated by a third-party device, which may be embedded within the device software (see NOTE within this section, below) or having an interface port for a third-party device to authenticate the media. This integrity check will provide a means for field testing the software to identify and validate the program. The test laboratory, prior to device approval, shall approve the integrity check method.

NOTE: If the authentication program is contained within the device software, the manufacturer must receive written approval from the test laboratory prior to submission. In addition, the manufacturer must provide a means to extract the program from the device. This shall include all hardware and software needed to perform this function.

4.8   Ticket Printers

4.8.1   General Statement. A ticket produced by a kiosk shall contain the following printed information at a minimum:

    a) Casino name/Site identifier;

    b) Machine number (or cashier number if supported);

    c) Date and time (24Hr format);

    d) Alpha and numeric dollar amount of the ticket;

    e) Ticket sequence number;

    f) Validation number;

    g) Bar code;

    h) Type of transaction or other method or differentiating ticket types;

    i) Indication of an expiration period from date of issue or date and time the ticket will expire

In addition, to an approved system used to validate the payout ticket, the ticket information on the central system shall be retained at least as long as the ticket is valid at that location.

4.8.2   Printer location. The printer shall be located behind one (1) layer of lock. (e.g., require opening of the main door to access), but not in the logic area or the drop box.