STANDARD **S**ERIES

GLI-26:

Wireless Gaming System Standards

Version: 1.1

Release Date: January 18, 2007

This Page Intentionally Left Blank

ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International, Inc.** 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 evidencing the certification to this Standard.

Wireless Gaming Systems

GLI-26 Revision 1.1

Initial internal draft release date 7/12/06 V1.0
Draft release for comment date 10/12/06 V1.0
Final release 01/18/07 V1.1

REVISION HISTORY

Document has been updated to reflect comments received from initial peer review on 7/24/06.
Document has been updated to revision 1.0, initial release incorporating comments received on 10/05/06.
Document has been updated to revision 1.1, incorporating comments received from initial release to the industry 01/18/07.

Table of Contents

Table of Figures and Tables

CHAPTER 1

1.0 OVERVIEW – TECHNICAL STANDARDS FOR WIRELESS GAMING SYSTEMS (WGS)

1.1 Introduction

1.1.1 <u>*General Statement*</u>. **Gaming Laboratories International, Inc. (GLI)** has been testing gaming equipment since 1989. Over the years, we have developed numerous standards for jurisdictions all over the world. In recent years, many jurisdictions have opted to ask for technical standards without creating their own standards. In addition, with technology changing almost monthly, new technology is not being incorporated quickly enough into existing standards due to the long process of administrative rulemaking. This document, *GLI Standard 26*, will set forth the technical Standards for Wireless Gaming Systems.

1.1.2 <u>*Document History*</u>. This document is an essay from many standards documents from around the world. We have taken each of the standards' documents, merged each of the unique rules together, eliminating some rules and updating others, in order to reflect both the change in technology and the purpose of maintaining an objective, factual standard. We have listed below, and give credit to, agencies whose documents we reviewed prior to writing this Standard. It is the policy of **Gaming Laboratories International, Inc.** to update this document as often as possible to reflect changes in technology, testing methods, or cheating methods. This document will be distributed FREE OF CHARGE to all those who request it. This standard and all others may be obtained by downloading it from our website at www.gaminglabs.com or by writing to us at:

Gaming Laboratories International, Inc.
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

1.2 Acknowledgment of Other Standards Reviewed

1.2.1 *General Statement*. These Standards have been developed by reviewing and using portions of the documents from the organizations listed below where applicable. We acknowledge all that have assembled these documents and thank them:

a)   Draft Mobile Gaming System and Standard Policies; (Nevada)

b)   IEEE 802.11(x) Standard

c)   GLI-11- Gaming Devices in Casinos

d)   GLI 13 - On-Line Monitoring and Control Systems

e)   GLI 21 - Server-Based Game Download Systems

f)   White paper, "Building Global Security Policy for Wireless LANS." Aruba Networks.

g)   "IPsec Virtual Private Network Fundamentals" by James Henry Carmouche (ISBN: 1587052075).

h)   Internet resources.

1.3 Purpose of Technical Standards

1.3.1 *General Statement*. The Purpose of this Technical Standard is as follows:

a)   To eliminate subjective criteria in analyzing and certifying Client Terminal game operation and system side components.

b)   To only test those criteria that impact the credibility and integrity of wireless gaming devices from both the Revenue Collection and Player's play point of view.

c)   ***To create a standard that will ensure the integrity of the wireless gaming system is equivalent to a wired system.***

d)   To distinguish between local public policy and laboratory criteria. At GLI, we believe that it is up to each local jurisdiction to setup their own public policy with respect to the wireless network.

e)   To recognize that non-gaming testing (such as Electrical and Product Safety 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 and allow for new technology to be introduced.

g)   To construct a standard that does not specify any particular 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.

1.3.2   *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.

1.4   Other Documents That May Apply

1.4.1   *General Statement*. The following other GLI standards may apply, depending on the features of the ETGS and references throughout this document. All GLI standards are available on our website at www.gaminglabs.com:

a) GLI-11 Gaming Devices in Casinos;

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

c) GLI-16 Cashless Systems in Casinos;

d) GLI-17 Bonusing Systems in Casinos; and

e) GLI-18 Promotional Systems in Casinos.

f) GLI-21 Server-Based Game Download System

1.5 Defining Wireless Gaming Systems

1.5.1   *General Statement*. A Wireless Gaming System (WGS) can be defined as any system composed of at least four components, outlined in Figure 1. A typical system consists of one or more client terminals; one or more access points (AP); a secure gateway/mobility controller, and a secure authentication server. Figure one depicts the architecture for a typical centralized system. The client and the AP communicate wirelessly using radio frequency (RF) waves over a private and secure, encrypted radio channel. The AP is typically connected to a secure

gateway/mobility controller via Ethernet or fiber optics. The secure gateway/mobility controller is connected to an authentication server typically using Ethernet or fiber optic cabling as well. The definitions given in the Glossary are typical of the components characterized in Figure 1.

1.5.2   <u>*Wireless Interface*</u> The interface defines the communication boundary between two entities, such as a piece of software, a hardware device, or the end-user. It may also provide a means of translation between entities, which do not speak the same language. This section deals with software interfaces, which exist between separate hardware and software components that ultimately compose of the wireless system, and provide a programmatic mechanism by which these components can communicate.

These software components are typically found in a Virtual Private Network (VPN). A VPN is a private communications network often used to communicate confidentially over a publicly accessible network. A VPN securely and privately transmits data over an unsecure and shared infrastructure, i.e. wireless networks. VPN's secure data that is transmitted across this common infrastructure by encapsulating, or encrypting the data, or both. In the context of VPN deployments, encapsulation is often referred to as tunneling, as it is a method that effectively passes data from one point on the network to another securely and, transparently across a shared network infrastructure. Generally, encryption implements the use of a mathematical operation usually referred to as an algorithm, or cipher, and the use of a key. It is the symmetric key, which is kept unknown to the would-be attackers. There are several different types of cryptographic keys, which are currently used with encryption. Other types of encryption include secure hashes and digital signatures. These encryption topics are outside the scope of this document, and should be researched further to determine which method is appropriate for each given scenario. However, the encryption key is the primary way of keeping the encrypted tunnel secure. Incorporating the appropriate data confidentiality capabilities into a VPN ensures that only the intended sources and destinations are capable of interpreting the original message contents. IPsec (Internet Protocol Security) is very effective at encrypting data using the Encapsulating Security Protocol (ESP). Utilizing ESP, IPsec manipulates readable text into encrypted data, or ciphered text. ESP manipulated messages are sent across the network in their ciphered representations, therefore, the original contents of the message are kept confidential from would be interceptors of the message.

IPsec-based VPNs represent one of the most secure and widely implemented types of VPNs available. However, IPsec is one of only many VPN technologies in existence today.

1.5.2.1 <ins>***General Statement***</ins>***:*** Wireless Gaming System (WGS) defined as:

A Client-Server System (CSS) which can be fragmentally defined as either, a Server Based Wireless Game Download System (SBWGDS) or a System Supported Game System (SSWGDS). Both of which can be defined as the combination of the Central Server(s), Client Terminals and all Interface Elements that function collectively for the purpose of linking the client terminal with the Central Server to perform the various functions related to wireless gaming, which may include, but are not limited to:

- Downloading of Game Logic to the Client Terminals;
- Server Based Random Number Generation;
- Thin and Thick Client Gaming Configurations.

The wireless client at a minimum will contain embodiment of randomness in determination of prizes, contain some form of activation to initiate the selection process, and contain a methodology for delivery of the determined outcome. The gaming device may be separated in parts, where some may be within or outside the client terminal (e.g., gaming devices that function with a system or server based RNG generation).

1.5.3 System Based Wireless Game Download System (SBWGDS) defined. The combination of a wireless server, a wireless client device, or a collection of client device(s) in which the entire or integral portion of game content resides on the server. This system works collectively in a fashion in which the gaming device will not be capable of functioning when disconnected from the system. The wireless client is in this system is typically referred to as a "Thin Client".

1.5.4 System Supported Wireless Game Download System (SSWGDS) defined.
The combination of a server and client terminal(s) which together allow the transfer of the entire control program and game content to the gaming device(s) for the purpose of downloading control programs and other software resources to the conventional gaming device or client terminal on an intermittent basis. The client terminals connected to the system are capable of operating independently from the system once the downloading process has been completed.

This configuration encompasses cases where the system may take control of peripheral devices or associated equipment typically considered part of a conventional gaming device such as a bill validator or a printer. In a System Supported Wireless Game, game outcome is determined by the client terminals connected to the system and not by the system itself. The gaming device is capable of functioning if disconnected from the system. The wireless client in this system is typically referred to as a "Thick Client".

Client: Any electronic gaming device with a secure wireless interface capable of being authenticated on the casino's private, wireless network. This section will address two similar, but functionally different types of client devices, thick and thin.

Thick Client: A thick client is a networked computer that performs the bulk of data processing operations itself, and relies on the server it is associated with primarily for data storage. This type of client has fairly strong processing abilities and is typically capable of being configured as a stand-alone device. A thick client usually has all of the software required to function as an independent entity on the network

Thin Client: A thin client is a networked computer, which typically lacks a hard drive. Ideally, this device will have only a screen, keyboard, and a pointing device (if needed). A Thin Client has just enough processing power to handle graphical and communication functionality. Thin client functionality is generally capable of displaying information provided by the application server. This type of client lacks application logic; therefore, it relies primarily on the server for data processing. This technology can be extended to include application software. For example, a web browser could be considered a thin client.

Devices that resemble Thick clients: BlackBerry PDA.

Devices that resemble Thin clients: A dumb terminal (VT100).

Access Point: Devices which act as hubs in a wireless network. Access points transmit and receive radio frequency waves to and from the client. Access Point's are typically wired to a secure gateway/mobility controller using Ethernet or a fiber optic link.

Secure Gateway/Mobility Controller: An electronic device that provides multi-layered (L1-L7) security. This device shall protect the air, the data, the users and the network it is connected to. The mobility controller provides the encryption and authentication services.

Server: A computer that provides client station access to information as a shared resource as part of that computer network. Depending upon the architecture chosen, (LDAP, RADIUS, Kerberos, or Microsoft Active Directory) users can be authenticated against a secure database.
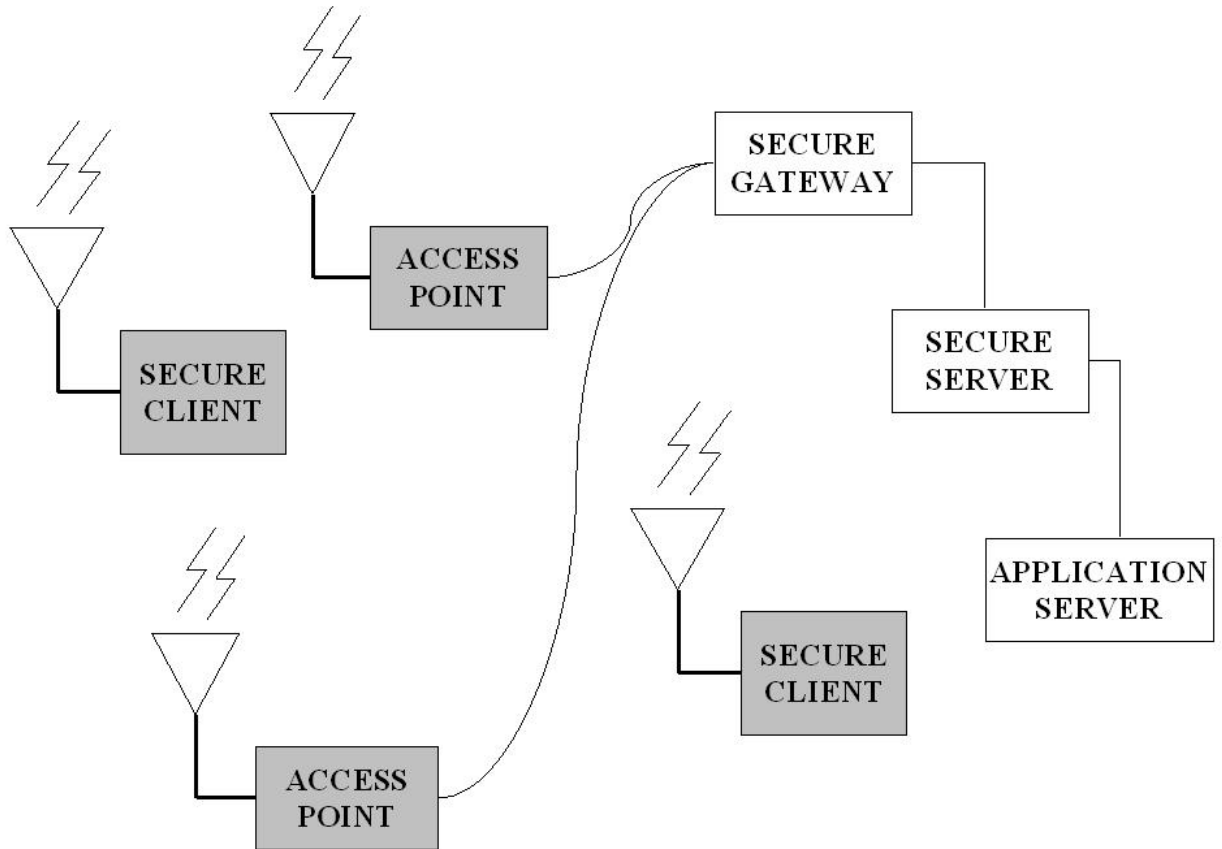
Figure 1: Typical Wireless System Block Diagram

1.6   Phases of Testing

1.6.1   <u>*General Statement*</u>. Wireless Gaming System submissions to the Test Laboratory will be performed in two phases:

a) Within the laboratory setting; and

b) On-site following the initial install of the system to ensure proper configuration of the security applications.

NOTE: In addition to the on-site testing of the system, the Test Laboratory shall provide training on this new technology to the local regulators, recommended field auditing procedures, and assistance with the compilation of Internal Controls, if requested.

GLI highly recommends the use of a private independent IT security company to plan, inspect and verify the integrity of the wireless gaming network.

CHAPTER 2

2.0 SUBMISSION REQUIREMENTS

2.1 **Refer to GLI-11 for Client Device Submission Requirements**

2.2 **Refer to GLI-13 for Server, Gateway Submission Requirements**

2.3 **Refer to GLI-16 for Cashless Systems Submission Requirements**

2.4 **Refer to GLI-21 for Server-Based Game Download Systems Submission Requirements**

CHAPTER 3

3.0 COMMUNICATION REQUIREMENTS

3.1 Introduction

3.1.1 General Statement. This chapter refers to the wireless communication link between the wireless client, the access point, the mobility controller and the wireless gaming server. This chapter will discuss the wireless communications protocol commonly known as 802.11(x) and will extend these methodologies to other wireless interfaces such as BlueTooth and infrared (IR). These alternate interface methods require special attention due to the limited functionality they offer.

3.1.2 Communication Protocol. Each component of a WGS must function as indicated by the communication protocol implemented. All communication between the server(s) and the mobile client must use appropriate authentication and cryptographic protocols to provide mutual authentication of the mobile unit and the server, ensuring the integrity of the data communicated, and for confidentiality, encrypting the data communicated. GLI strongly recommends the use of commercially available 802.1(x) protocol compliant devices in conjunction with other applicable security conscience components, which would ultimately make up the wireless gaming system. Any alternative implementations will be reviewed on a case-by-case basis, with regulator approval.

3.2 System Security

General Statement. In the event the WGS Server is utilized in conjunction with other systems; (i.e. On-Line Monitoring and Control Systems, Ticket Validation Systems, Progressive Systems, etc.) including remote access, all communications, must pass through at least one approved application-level firewall, and must not have a facility that allows for an alternate network path. One choice for network authentication is IEEE 802.1X. As an open standard with support for multiple authentication protocols, 802.1X is flexible enough to support everything from digital

certificates to username/password authentication, and platforms from low-end PDA devices and mobile phones up to desktop and server operating systems.

NOTE: Each wireless gaming system as submitted to the Test Laboratory will be examined thoroughly to ensure that the proposed field configuration is secure. The Test Laboratory may provide additional security recommendations and provide on-site training to the regulators, if requested. GLI recommends the use of a private independent IT security company to plan, inspect and verify the integrity of the wireless gaming network

3.2.1   *Wireless Gaming System Physical Security*   Wireless Gaming System shall:

Physically locate wireless access points that are not easily accessible to the general public.

If applicable, disable all exposed Ethernet outlets to reduce the risk of network intrusion.

Have an independent network for the wireless gaming system.

Monitor the client for evidence of physical entry into the device. If entry has been detected, the system shall assert controls such that, the game becomes locked and not playable.

Retain evidence of physical tampering.

Suspend the client from game play while the client is outside of the approved gaming area. When the client re-enters the approved gaming area, the system shall force the client to re-authenticate to resume game play.

Implement a time period, which is configurable for re-authentication.

GLI recommends using wireless solutions that meet or exceed the FIPS (Federal Information Processing Standard) 140 Level 2 standard. Any other alternative wireless solutions will be reviewed on a case-by-case basis, with regulator approval.

3.2.2   *Wireless Gaming System Security*   Wireless Gaming Systems shall:

Be designed or programmed in such a way, that it may only communicate with authorized wireless clients. Software transferred between server and client or conventional gaming devices of a system based game must be implemented using a method that securely links the client or clients to the server, such that the software may only be used by authorized clients. In general, if certificates, keys or seeds are used they must not be hard coded, and must change automatically,

over time, as a function of the communication link. Each method shall be reviewed by the jurisdiction and the lab on a case by case basis

Employ encryption and strong user authentication, with a recommendation of at least two methods of validation prior to opening a session.

Acceptable methods are : Username and password, a physical token, smart ID card, or non-alterable biometrics measurements. Some examples of non-alterable biometric techniques include identity recognition, iris scan, voice recognition and digital fingerprints.

Always perform mutual authentication to ensure that clients only communicate with valid

networks. One example of this type of authentication is done using a digital certificate. Upon joining the network, the client is presented with a server-side digital certificate. If the client trusts the certificate, the authentication process will continue. If the certificate is not trusted, the process will terminate and the client shall enter a locked condition requiring attendant intervention to clear.

Validate clients at pre-defined time intervals with at least one method of authentication as described above. This time interval shall be configurable based on jurisdictional requirements.

Maintain a list (database) of authorized devices, which it can communicate with. This list shall include the device name, a unique device ID and the corresponding hardware identifier (MAC).

Install and maintain a stand-alone stateful packet inspection firewall, which shall isolate the access points from other network components that the casino has deployed.

Not broadcast (hide) their Service Set Identifier (SSID).

GLI recommends implementing MAC (Media Access Control) filtering to prevent unauthorized users from gaining access to the wireless network.

Close active sessions because of the following:

> User authentication has exceeded the number of failed attempts; the number of failed attempts shall be configurable based on jurisdictional requirements.

> No game activity has occurred within the specified time limit as configured by the jurisdiction.

> The mobile unit has been disabled due to physical boundary restrictions.

> The user or the system has terminated the session.

> Ignore any device that is not approved to be on the wireless network.

Provide a printable report of failed network access attempts, including the time and date stamp, the device name, and the hardware identifier of all devices requesting access to the network.

Suspend the client from game play while the client is outside of the approved gaming area. When the client re-enters the approved gaming area, the system shall force the client to re-authenticate to resume game play.

Implement a method that securely links the wireless communications device to the wireless gaming system as authorized to communicate over that link.

Provide the capability for the administrator to disable the client device at anytime.

GLI recommends the use of strong user authentication, authorization and encryption, which will validate the user against a secure database. Communications between the system and the client device shall use protocols designed for securing, authenticating and encrypting wireless networks. Examples of the appropriate protocols are IEEE 802.1x; because it provides the framework required; thus, permitting the use of higher-level authentication methods such as, the methods listed in the Table 1. 802.1X provides support for Extensible Authentication Protocol (EAP) types which allows network administrators to choose from several different authentication methods for wireless clients and servers.

802.1x RECOMMENDED AUTHENTICATION METHODS		
AUTHENTICATION METHOD	ACRONYM	AUTHENTICATED AGAINST
Protected Extensible Authentication Protocol	PEAP	LDAP, RADIUS, Kerberos or Microsoft Active Directory servers, as well as local databases stored on the secure gateway controller. *Definitions are listed at the end of this document in the Glossary.*
Extensible Authentication Protocol-Transport Layer Security	EAP-TLS	
Extensible Authentication Protocol-Tunneled Transport Layer Security	EAP-TTLS	
Virtual Private Network with L2TP/IPsec	VPN	
Point to Point Tunneling Protocol	PPTP	
Secure Sockets Layer	SSL	

Table 1: Recommended authentication methods for use with 802.1x

Although, an intruder can monitor the communication link over the air, the data inside the encrypted tunnel cannot be intercepted by implementing methods listed in Table 1.

It is not recommended to use non-tunneled EAP methods listed in Table 2, because wireless data links could be compromised.

8021.x NON-RECOMMENDED AUTHENTICATION METHODS	
AUTHENTICATION METHOD	ACRONYM
Extensible Authentication Protocol	EAP
Extensible Authentication Protocol Message Digest 5	EAP-MD5
Lightweight Extensible Authentication Protocol	LEAP

Table 2: Non-recommended authentication methods for use with 802.1x

3.2.3 *Wireless Gaming Client*. Wireless Gaming Clients shall:

Be designed or programmed in such a way, that it may only communicate with authorized Wireless Gaming Systems as defined in section **1.5**.

Employ strong user authentication requiring at least two methods of validation prior to the opening of a secure session. Acceptable methods are as follows, username and password, a physical token, or biometrics measurements.

Utilize a public encryption algorithm, GLI recommends AES (Advanced Encryption System), or 3DES (Data Encryption Standard). Other shall be reviewed on a case by case basis.

Only operate as a wireless gaming client within the approved areas of game play as determined by jurisdictional regulations.

Notify the patron once the client device leaves the approved gaming area, and

Suspend game play while the client is outside of the approved gaming area, even though wireless coverage still may exist.

Force the client to re-authenticate when the client re-enters the approved gaming area.

Return to the last known game state prior to being suspended.

3.2.4 ***Firewall Audit Logs***. The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

      a) all changes to configuration of the firewall;

      b) all successful and unsuccessful connection attempts through the firewall; and

      c) the source and destination IP Addresses, Port Numbers and MAC Addresses.

3.3   Remote Access

3.3.1 ***General Statement***. Remote Access is defined as any access to the system outside of the internal network. Remote Access, where permitted, shall authenticate all computer systems based on the authorized settings of the WGS or firewall application that establishes a connection with the WGS. The security of Remote Access will be reviewed on a case-by-case basis, in conjunction with the current technology and approval from the local regulatory agency. The following are additional requirements:

a) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);

b) No unauthorized access to any database other than information retrieval using existing functions; and

c) No unauthorized access to the operating system.

NOTE: GLI acknowledges that the system manufacturer may, as needed, remotely access the WGS and its associated components for the purpose of product and user support, if permitted.

3.3.2 ***Remote Access Auditing***. The WGS Server must maintain an activity log either automatically or have the ability to manually enter the logs depicting all Remote Access information that includes the:

a) Log on Name;

b) Time and date the connection was made;

c) Duration of connection; and

d) Activity while logged in, including the specific areas accessed and changes that were made.

CHAPTER 4

4.0 WIRELESS CLIENT REQUIREMENTS

4.1 **Refer to GLI-11 for Client Device Requirements**

4.4.1 <u>***General Statement***</u>: The Client device portion of the Wireless Gaming System shall comply with the technical standards outlined in GLI-11, *where applicable*. In addition to GLI-11, the client device shall meet the following minimum requirements.

a) Include pay tables and patron help screens, which include the rules associated with the operation of the wireless client.

b) Shall have sufficient redundancy and modularity to accommodate a component failure. If a component failure is detected the wireless gaming device shall cease operation. In addition, there shall be redundant copies of each audit log locally and on the system database.

c) Retain evidence of physical tampering. Physical locks and seals are acceptable methods.

d) Enter a locked state immediately after unauthorized physical entry is detected, and

e) Report illegal entry to the system, where applicable, and require an attendant to clear the locked condition caused by illegal physical entry into the device.

f) Purge cached user authentication information at the termination of each session.

g) *Where applicable*, utilize a random number generator, which passes the technical requirements as outlined in GLI-11: "Gaming Devices in Casinos".

h) *Where applicable*, comply with the technical requirements as outlined in GLI-21: "Server-Based Game Download Systems".

i) *Where applicable*, comply with the technical requirements as outlined in GLI-16: "Cashless Systems in Casinos".

CHAPTER 5

5.0   WGS SERVER REQUIREMENTS

5.1   Introduction

5.1.1   General Statement. This chapter describes the WGS requirements pertaining to the WGS Server where it may be used locally and applies only to the download of any game content from the WGS Server to the wireless client terminal. Downloadable content shall be evaluated against GLI-21: Server-Based Games Download Systems. In the case where the WGS Server also performs tasks as required by other systems, (i.e. On-Line Monitoring and Control System, Ticket Validation System, etc) those portions shall not apply to this document and will be evaluated against the appropriate standard.

5.2   System Failure

5.2.1   General Statement. The WGS shall have sufficient redundancy and modularity to accommodate a component failure to prevent the interruption of the WGS operations. In addition, there shall be redundant copies of each audit log and system database, where applicable, on the WGS Server with open support for backups and restoration. This includes a WGS that has support for failover redundancy. Backup scheme implementation must occur at least once every day, although all methods will be reviewed on a case-by-case basis by the testing laboratory.

5.2.2   Recovery Requirements. In the event of a catastrophic failure when the WGS cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information, where applicable:

a) Significant events.

b) Auditing information.

c) Specific site information such as game configuration, security accounts, etc.

5.3   Self Monitoring

5.3.1   General Statement. The WGS must implement self monitoring of all critical Interface Elements (e.g. Central hosts, network devices, firewalls, links to third parties, etc.) and shall have the ability to effectively notify the system administrator of the condition, provided the condition is not catastrophic. The WGS shall be able to perform this operation on demand and with a frequency of at least once in every 24-hour period. All critical interface elements will be reviewed on a case per case basis and may require further action by the system depending upon the severity of the failure.

5.4   WGS Software Verification

5.4.1   General Statement. Each component of the WGS must have a method to be verified via a third-party verification procedure. In addition, the WGS shall have the ability to:

a) Authenticate all critical files including, but not limited to, executables, data, operating system files and other files, which may affect the game outcome or operation, which reside on the medium.

b) Employ a third-party industry standard secure hashing algorithm. (eg. MD5 or SHA1) The algorithm shall use a key or seed of sufficient length and complexity. The manufacturer should be prepared to demonstrate the algorithm choice to both the testing laboratory and jurisdiction.

c) The third-party verification process shall not include any process or security software provided by the operating system manufacturer. A secondary check may use commercially available software by the operating system manufacturer as part of the secondary verification.

d) The WGS Server must be capable of verifying that all control programs are authentic copies of approved games.

e) For System Supported Wireless Game Download Systems, the game program must be checked in its entirety at the client terminal and at the server after the client terminal has been powered up. In the event of failed authentication the Client terminal and the server should immediately enter an Error Condition with the appropriate audio and visual indicator, and record the details, including time and date of the error in a log. This error shall require operator intervention.

f) In the event of a failed authentication after the player terminal has been powered up, the client terminal; should immediately enter an Error Condition with the appropriate audio and visual indicator, and record the details, including time and date of the error in a log. This error shall require operator intervention. The game shall display specific error information and shall not clear until the file authenticates properly, or following operator intervention, or the medium is replaced or corrected, and the device's memory is cleared, the game is restarted, and all files authenticate correctly.

5.5   Game Program Library

5.5.1   _General Statement_. Where applicable, the Game Program Library shall only be written to, with secure access that is controlled by the regulator, in which case the manufacturer and/or operator will be able to access the Game Program Library. The deletion of games from the program library is acceptable provided it meets all the requirements defined in section 5.5.2.

5.5.2   _Audit Log_. Any changes that are made to the Game Program Library, including the addition, changing or deletion of Game Programs, must be stored in an non-alterable audit log, which shall include:

a) Time and Date of the access and/or event;

b) Log In Name;

c) Game Program ID Numbers added, changed, or deleted;

d) The Player Terminal(s) which the Game Program was downloaded to and, if applicable, the program it replaced; and

e) Changes to the Player Terminal configuration settings and what the changes were.

5.6   Download of Client Terminal Control Programs

5.6.1   _General Statement_. This chapter will outline the requirements for a client device that is used in a WGS environment that are in addition to the GLI-11 Gaming Devices in Casinos regulations, except where noted.

5.6.2 *Control Program*. This section will detail the minimum technical standards that shall be met, where applicable, when downloading the Client Terminal Control Program from the Wireless Gaming Server to the Client Terminal, provided the process does not adversely affect the game operation:

a) Below are the methods to store the current game data that is pertinent to the individual Player Terminal when updating the Control Program*:

1. Where applicable, the Game Data is uploaded and securely stored on the Wireless Gaming Server and is maintained for a minimum of 24-hours and archived after that time; or is maintained in log or script file. If this method is used, the process in downloading the new Control Program to the Player Terminal must ensure that all critical areas of memory are overwritten by a default value; or

2. If the Wireless Gaming Server is not capable of meeting the above regulation, Regulatory Controls may be required from the GDS Server for new Player Terminal Control Program downloads. In addition, the alternate methods used will be reviewed by the Test Laboratory and the Regulator on a case-by-case basis.

    *Please note it must be possible to perform a forensic analysis of the game which includes viewing the game data and being able to place it onto a comparable device for evaluation.

b) Prior to execution of updated software, the Player Terminal must be in an Idle State and the software is successfully authenticated, as defined within item 4.6.2, Verification of Control Program.

5.7   Control of Client Terminal Configurations

5.7.1 *General Statement*. Client terminals used in a Wireless Gaming environment that have alterable configurations that require Regulatory Control, as outlined within GLI-11, may be optional, provided that the rules within this section are met.

5.7.2 Paytable/Denomination Configuration Changes. Client terminal Control Programs that offer multiple paytables and/or denominations that can be configured via the Wireless Gaming Server will not require Regulatory Control to change the paytable selected, provided:

a) All paytables that are available meet the local theoretical payback percentage and odds requirements, where applicable;

b) The client terminal maintains the Amounts Bet and Amounts Won meters within Critical Memory for each of the paytables that are available;

c) The client terminal maintains the Master Accounting meters in dollars and cents or the lowest denomination available for the local currency;

d) The game is in an Idle State when the update occurs; and

e) The change will not cause inaccurate crediting or payment.

5.7.3 Client terminal RAM Clear. The process of clearing RAM on the client terminals via the Wireless Gaming server must utilize a secure method that would require Regulatory Control. For systems that do not comply with this rule, the regulator shall approve the method used.

5.8 Download of Random Values

5.8.1 General Statement. This section governs elements of a Wireless Gaming Server that may be utilized for the generation of Random Values, which are subsequently communicated to the client terminal's Control Program that is required for the determination of game outcomes. The GDS Server generation of Random Values does not include the generation of game outcomes[1].

5.8.2 Random Number Generator. In the event the Wireless Gaming Server has the ability to download Random Values to the client terminal, the Random Number Generator shall function, as outlined within the RNG Requirements of GLI-11 section VI.

---

1 Systems utilizing finite pools of game outcomes (i.e., Electronic Pull-Tab Systems) shall conform to the GLI-14 Finite Scratch Ticket and Pull-Tab Systems, in addition to the standards set forth herein, where applicable.

Glossary

Reference	Definition
WGS Server	The 'host' computer that is one source of the system controls and information.
Control Program	The control program is the software that operates the Player Terminals functions, including the paytable(s) for the game. The Control Program can run independently of the GDS or may require information generated by the system to perform the Player Terminal functions.
Critical Memory	Critical memory is used to store all data that is considered vital to the continued operation of the gaming device. Please refer to GLI-11 Gaming Devices in Casinos, rule 3.13 Contents of Critical Memory for further information.
Firewall	Network security barrier. A firewall is a device that guards the entrance to a private network and keeps out unauthorized or unwanted traffic.
Game Contents	The downloading of any data, with the exception of the Game Program or Random Values.
Game Data	The data stored within non-volatile memory that reflects the accounting and security events that is specific to the individual Player Terminal, which includes: 1) Error Logs. 2) All Drop Meters. 3) Last Game Recall (this should be maintained within the game history in the event there is a player dispute where the suggested problem took place earlier and was not reported until after the update of the new game). 4) Bill Recall. 5) Cashless Transaction Logs. 6) Audit Logs for the Player Terminal Game Program transactions.
Game Program	The control program that resides at the GDS server and/or the player terminal
Program Library	A Regulator controlled library that resides at the GDS server that contains the complete game program and/or the server side critical components of a game program.
Idle State	The Player Terminal is in an Idle State, including while the game is disabled, when there is no activity on the device, no credits, no player's card, and no Error Conditions.
Player Terminal	An element within a WGS that is a gaming device.
Random Values	Where a Random Number Generator is stored on the GDS Server, and communicates random numbers to the Player Terminal(s) that are required for the Player Terminal to function, where the Player Terminal's Control Program is not independent of the GDS Server.
Regulatory Control	A method used by and is only accessible to the regulator to ensure the security of the GDS.
GDS	A Server-Based Game Download System (GDS) is the combination of a GDS Server, Player Terminals and all Interface Elements that function collectively for the purpose of downloading Player Terminal Game Content from the GDS Server to the Player Terminal(s), which may include: 1) The Player Terminal Control Program; and/or 2) Randomly Generated Values; and/or 3) Other Game Content that is generated by the GDS Server and downloaded to the Player Terminal for the operation of the game.
EAP	Extensible Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol- Tunneled Transport Layer Security
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
RADIUS	Remote Authentication Dial In User Service
Kerberos	A network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

Active Directory	**Active Directory** is an implementation of LDAP directory services by Microsoft for use in Windows environments
SSID	Service set Identifier, Network name
SAWGD	Stand Alone Wireless Gaming Device.
SSWGD	System Supported Wireless Gaming Device.
Biometrics	Technologies for measuring and analyzing physical characteristics such as fingerprints, eye retinas and irises, voice patterns facial patterns, and hand measurements, especially for security and authentication purposes.