

Alcohol and Gaming Commission
of Ontario

**Server-Assisted and
Server-Based Gaming
Minimum Technical
Standards**

Version 1.0
April 2010

Table of Contents

INTRODUCTION	4
SERVER-ASSISTED AND SERVER-BASED GAMING MINIMUM TECHNICAL STANDARDS	5
1 SECURITY	6
1.1 <i>Physical Security of the Server</i>	6
1.2 <i>Security of Network</i>	6
1.3 <i>Logical Security of Communication</i>	7
1.4 <i>Server Access Control</i>	8
1.5 <i>Software Integrity and Security</i>	10
2 AUTHENTICATION	11
2.1 <i>Self-Authentication of Gaming Software on the Server</i>	11
2.2 <i>Self-Authentication of Gaming Software on the Server-Assisted Slot Machine and Client Station</i>	11
2.3 <i>Field Authentication of Software on the Server</i>	13
2.4 <i>Field Authentication of Software on the Server-Assisted Slot Machine and Client Station</i>	13
3 BACKUP AND RECOVERY	14
3.1 <i>Data Backup</i>	14
3.2 <i>Archive/Data Warehouse</i>	14
3.3 <i>Server-Based Server Backup</i>	14
4 SOFTWARE DOWNLOAD AND INSTALLATION	15
4.1 <i>Scheduling Software</i>	15
4.2 <i>Change Controls</i>	15
4.3 <i>Slot Machine Requirements for Download and Installation</i>	16
4.4 <i>Operational Requirements for Download and Installation</i>	18
5 ERROR CONDITIONS	20
6 METERS	21
7 REPORTS AND LOGS	22
7.1 <i>Server Requirements for Reports and Audit Logs</i>	22
7.2 <i>Server-Assisted Slot Machine and Client Station Requirements for Reports and Audit Logs:</i>	23
7.3 <i>General Requirements for Reports and Audit Logs:</i>	24
8 REMOTE ACCESS	26
8.1 <i>Remote Access to Server-Assisted or Server-Based Slot Systems</i>	26

9	FORENSIC CAPABILITIES.....	27
10	OTHER REQUIREMENTS	28
11	COMPLIANCE WITH AGCO'S ELECTRONIC GAMING EQUIPMENT MINIMUM TECHNICAL STANDARDS.....	29
	GLOSSARY	30

Introduction

The Registrar of Alcohol and Gaming is appointed under the *Alcohol and Gaming Regulation and Public Protection Act, 1996* and has powers and duties under the *Gaming Control Act, 1992* and its regulations. The Registrar has the power and duty to approve gaming equipment and gaming management systems pursuant to Section 21 of Ontario Regulation 385/99. The Registrar has specified the following standards as the minimum standards to be used in assessing server-assisted and server-based gaming equipment and gaming management systems for approval. The Registrar has delegated to the Deputy Registrar the authority to make decisions on approval of gaming equipment and gaming management systems.

The intent of this document is to set minimum technical standards for server-assisted and server-based gaming with regards to the technical integrity, safety and security of the equipment or the system, including its accounting capability, and the integrity of the games of chance held at the gaming premises per Ontario Regulation 385/99, Sections 15(a) and 21(4)(a).

Modifications to the Technical Standards Document

From time to time it may be necessary to make modifications to this document in order to address the following:

- a) Changes in technology;
- b) Changes, deletions or additions to meet the intent described above;
- c) Introduction of new equipment where no standards have been set;
- d) Rephrasing of a particular standard(s) to provide better clarification.

Treatment of Approved Gaming Equipment and Systems

Gaming equipment and systems that were approved prior to these standards may remain in the field unless they are used for server-assisted or server-based gaming in which case these technical standards must be met.

Operational Requirements

These standards do not deal with implementation requirements at the gaming premises such as access to the server room. These requirements will be dealt with through the internal control procedures for each gaming establishment.

Assumptions

It is assumed that standard industry practices will be applied (standard software development practices, design and development including handling of abnormal operations, etc.). Therefore, they are not included in these standards.

Server-Assisted and Server-Based Gaming Minimum Technical Standards

1 Security

1.1 Physical Security of the Server

The implementation plan of all requirements listed in this section must be submitted by the operator to the Registrar prior to installation or any subsequent changes made to the plan.

- 1.1.1 A slot machine server must be located in a “slot machine server room”, a secure area with restricted access approved by the Registrar. The slot machine server room must be readily accessible to AGCO personnel twenty-four hours a day. Nothing herein shall be deemed to preclude the location of a slot machine server room, with prior approval from the Registrar, in a secure area with restricted access that contains computer system components for more than one gaming premises, or more than one computer system.
- 1.1.2 A slot machine server must be capable of being maintained in a locked computer rack or other secure area approved by the Registrar in the slot machine server room. Physical access to the slot machine server must be controlled by two different locks.
 - a) The key to the first lock must be under control of gaming key employee(s) that are authorized by the Registrar and not responsible for maintaining the slot machine server (e.g. IT Manager, Director or security personnel that are registered by the AGCO under the Gaming Control Act).
 - b) The key to the second lock must be held in an AGCO-sealed locked box in the IT server room, under surveillance coverage, accessible by a representative of the Registrar as well as the gaming key employee(s) not responsible for maintaining the slot machine server and authorized by the Registrar to access the key in the case of emergency when the representative of the Registrar is unavailable. The site must notify the representative of the Registrar any time the key to the second lock is accessed by the gaming key employee(s).
 - c) Other methods to secure the key to the second lock may be considered and approved by the Registrar.

1.2 Security of Network

- 1.2.1 The proposed network design that meets all requirements listed in this section must be submitted by the operator to the Registrar prior to implementation.
- 1.2.2 Communication between a slot machine server and a server-assisted slot machine or client station must be conducted over a secure hard-wired network.
- 1.2.3 Communication between the server-assisted or server-based slot system and any other on-site computer system must be conducted over a secure hard-wired network.
- 1.2.4 Communication between a slot machine server and a server-assisted slot machine or client station must be conducted over either:
 - a) A dedicated, physically secured network, or
 - b) A secured communication path that:
 - i. Is dedicated to communication between gaming equipment and gaming management systems approved by the Registrar;

- ii. Authenticates the communicating systems;
- iii. Ensures data confidentiality; and
- iv. Prevents third party interception or corruption of communicated signals,

unless otherwise approved by the Registrar.

1.2.5 Communication between the server-assisted or server-based slot system and any on-site or off-site gaming management system approved by the Registrar must be conducted over either:

- a) A dedicated, physically secured network, or
- b) A secured communication path that:
 - i. Is dedicated to communication between gaming management systems approved by the Registrar;
 - ii. Authenticates the communicating systems;
 - iii. Ensures data confidentiality; and
 - iv. Prevents third party interception or corruption of communicated signals,

unless otherwise approved by the Registrar.

1.2.6 If secured communication paths are used to satisfy 1.2.4 or 1.2.5, the gaming site operator must provide to the Registrar the results from an independent (an outside firm that has recognized expertise in network security) audit of network security of the implemented network. This audit must be provided to the Registrar before the server-assisted or server-based slot system is made available for patron play following initial implementation and thereafter following any subsequent changes made to the system. The security audit must ensure that the server-assisted or server-based slot system satisfies the requirements of this section and is secured against intrusion or tampering from other systems or sources from outside of the secured communication paths described in this section, and that logical security controls are in place to prevent unauthorized access to the network.

1.3 Logical Security of Communication

1.3.1 Transfers of software between a slot machine server and a server-assisted slot machine or client station must be conducted using MD5 message digest validation and SSL digital certificates, or an equivalent or better methodology as accepted by the Registrar. The network must securely link the slot machine server to the server-assisted slot machine or client station so that the software can only be transferred to and used by an authorized server-assisted slot machine or client station

1.3.2 A server-assisted or server-based slot system must not alter any component of the system that would interrupt, or affect the function or operating parameters of a game in progress on any other server-assisted slot machine or client station.

1.3.3 Prior to and while transferring software or data to a server-assisted slot machine or client station, a slot machine server must, at a minimum:

- a) Authenticate the identity of the server-assisted slot machine, client station or other device to which the software or data is transmitted;
- b) Ensure that all software and data transmitted is completely and accurately received; and
- c) Detect the presence of corrupt or lost data packets and, as necessary, repeat the transmission or abandon and log the failed attempt.

- 1.3.4 Transmitted information between the components in a server-assisted or server-based slot system related to player input, game outcome, financial transactions, and game recall information must be encrypted using an asymmetrical encryption algorithm with a 512 bit key or another methodology as accepted by the Registrar.
- 1.3.5 Notwithstanding the provisions of section 8, Remote Access, a server-assisted or server-based slot system must only communicate with equipment or programs external to the server-assisted or server-based slot system through a secure interface. This interface will specifically not allow any external connection to directly access the internal components, software or data of the server-assisted or server-based slot system. The interface must:
- a) Be based on a specific defined protocol or a specific set of defined commands and as a result of these commands, retrieve information for an external request;
 - b) Place data in an area sufficiently segregated from the server-assisted slot machine, client station or server software that is available to external requests or associated equipment; or
 - c) Be of a suitable design capable of supplying requested information while isolating the external request or equipment from the server-assisted slot machine's or client station's internal components, software or data.
- 1.3.6 Any connection to the system, with the exception of on-site slot management systems and gaming equipment approved by the Registrar, must, at minimum, include a hardware and software firewall that satisfies the following requirements:
- a) Administrative access to the firewalls must be limited to authorized employees only;
 - b) The firewall application must maintain an audit log of all changes to the configuration of the firewall, all connection attempts, successful and unsuccessful, through the firewall and the source and destination IP addresses, port numbers and MAC addresses;
 - c) The firewall applications must disable all communications and generate an error event if the audit log becomes full. The audit log must be retained for a minimum of thirty days or as approved by the Registrar; and
 - d) A selectable parameter, "unsuccessful connection attempts" may be utilized to deny further connection requests should the predefined threshold be exceeded. The system administrator must also be notified when connection requests are denied.
- 1.3.7 All server computers, routers and other slot system components exposed to external communications must use firewall protection and be compliant with the provisions of section 1.3.6 above.

1.4 Server Access Control

- 1.4.1 Each computer system that has access rights to a slot machine server in a server-assisted or server-based slot system must utilize a secure and trusted means of communication as approved by the Registrar that is equivalent or better than issuance of digital certificates by the slot machine server. The security method must conduct a check to ensure that the network remains secure and trusted whenever:

- a) Any casino computer system (such as a slot monitoring system, accounting system or gaming voucher system) is connected to the server-assisted or server-based slot system;
 - b) A software program, file or data is transmitted to the casino computer system;
 - c) On start-up or reboot of the server, or on demand; and
 - d) At minimum, randomly once every twenty-four hours.
- 1.4.2 Access to any slot machine server data which is not transferred pursuant to 1.2.5 and 1.3.5 above must be by way of a data warehouse or similar scheme as approved by the Registrar and not by the slot machine server itself. The interface between the data warehouse and the slot machine server must comply with sections 1.2.5, 1.3.5 and 1.4.1.
- 1.4.3 Except as otherwise authorized by the Registrar, critical software and computer files must be controlled only from the slot machine server through the downloaded server-assisted slot machine or client station software, and must not be controlled at or by any of the individual server-assisted slot machines or client stations connected to the slot machine server or at or by any other gaming management system or device. Any critical slot machine program or computer file that is not controlled by the slot machine server must be authenticated and sealed by the AGCO. The operator's procedures for controlling such programs must, at a minimum, require:
- a) The presence of an AGCO representative whenever such critical slot machine programs or computer files are installed, modified, configured or deleted;
 - b) Compliance with the applicable log files of sections 7, Reports and Logs below; and
 - c) Compliance with section 4.3.4 below, regarding changes to slot machine games and options.
- 1.4.4 The slot machine server must provide for adequate and effective control of logical access to the server and, at a minimum, must be capable of assigning rights and privileges to each user, including the following requirements:
- a) Allowance for the secure administration of a unique system account for each user to provide an adequate segregation of duties in accordance with the provisions of Electronic Gaming Equipment Minimum Technical Standards sections 5.4.1, 5.4.3, 5.4.4, 5.4.5 and 5.4.6 as applicable;
 - b) Use passwords that contain at least six alphabetic and/or numeric characters and expire no more than 90 days after creation;
 - c) Use passwords that are stored in an approved encrypted form so that the original passwords cannot be exposed for unauthorized use;
 - d) Use appropriate access permission to restrict unauthorized users from viewing, changing, or deleting critical files and directories;
 - e) Immediately disallow any further attempts to access the system following no more than five consecutive failed attempts within no less than 30 minutes by a user account to obtain access to the system, by automatically disabling the user account;
 - f) Require the user name and password of at least two employees, or the use of split passwords or an other method approved by the Registrar that ensures the presence and participation of at least two individuals, prior to providing access to files and directories containing critical software or any other sensitive data; and

- g) Automatically monitor and record access by any person to files and directories containing critical and sensitive data.

1.5 Software Integrity and Security

- 1.5.1 The slot machine server must utilize an encryption standard pursuant to Electronic Gaming Equipment Minimum Technical Standards section 1.1.2, for all critical software on the slot machine server. The server logs and database tables required in section 7, Reports and Logs, must also be protected from alteration after initial writing. Database tables need not be unalterable or write protected if they are secured in an alternate manner approved by the Registrar.
- 1.5.2 The outcome of each play on a server-assisted slot machine must be determined solely by the critical software activated on the individual server-assisted slot machine on which it is played, including its random number generator. A slot machine server must not be capable of altering any component of critical software on any connected server-assisted slot machine that would interrupt, or affect the functions, game outcome, or configurable options of a game in progress on any server-assisted slot machine connected to the slot machine server; provided however, that a slot machine server may stop a game or disable a server-assisted slot machine at any time if there is a valid reason to do so as approved by the Registrar.
- 1.5.3 The outcome of each play on a client station must be determined solely by the critical software located on the slot machine server, including its random number generator. A slot machine server must not be capable of altering any component on any connected client station that would interrupt or affect the functions, game outcome, or configurable options of a game in progress; provided however, that a slot machine server may stop a game or disable a client station at any time if there is a valid reason to do so as approved by the Registrar.

2 Authentication

2.1 Self-Authentication of Gaming Software on the Server

- 2.1.1 The critical software stored on alterable storage media that will be installed on or used by a slot machine server must contain a message digest pursuant to Electronic Gaming Equipment Minimum Technical Standards section 1.1.1, Alterable Storage Media.
- 2.1.2 A slot machine server must automatically authenticate each message digest for every activated game using approved authentication software randomly every twenty-four hours and upon startup, software installation or update and on demand and must prevent the execution of any software program if the program or any portion thereof is determined to be invalid. A server-based slot machine server must also authenticate each message digest for every activated game on reboot of the server and must prevent the execution of any software program if the program or any portion thereof is determined to be invalid. This automatic authentication must be transparent and must not interfere with the normal operations at the server-assisted slot machine or client station.
- 2.1.3 The authentication mechanism must reside on and load from non-alterable media and a report must be available that details the authentication results for each control program component on both the server and the server-assisted slot machine or client station. The media will be inspected and physically sealed or otherwise secured by the AGCO.
- 2.1.4 If a message digest error (from 2.1.2 above) is detected:
- a) The slot machine server must provide notification of the error, including the associated invalid program or programs and/or the slot machine tilt, to the departments designated by the Registrar (e.g., MIS, Slots, Surveillance, Audit), where technically possible;
 - b) The server must be capable of automatically creating a report which must detail the date, time and outcome of the failed authentication, and identify the invalid program or programs; and
 - c) An AGCO representative, designated by the Registrar, must be immediately notified of any failed authentication.

2.2 Self-Authentication of Gaming Software on the Server-Assisted Slot Machine and Client Station

- 2.2.1 The critical slot machine game software that is downloaded and/or offered on a server-assisted or server-based slot system must contain a message digest pursuant to Electronic Gaming Equipment Minimum Technical Standards section 1.1.1, Alterable Storage Media.
- 2.2.2 The server-assisted slot machine or client station must contain an approved hardware device that:
- a) stores the authentication software in a secure manner and uses it to authenticate the message digest of all critical software downloaded to the server-assisted slot machine or client station from the server;
 - b) is an EPROM or other approved read-only storage media;

- c) is capable of being authenticated and physically sealed by the AGCO;
 - d) executes for all critical computer files each time the server-assisted slot machine or client station is powered up, and whenever files are loaded from the media; and
 - e) prevents further play of the server-assisted slot machine or client station if unexpected data or any inconsistencies are detected by immediately entering into a tilt mode pursuant to Electronic Gaming Equipment Minimum Technical Standards section 1.1.5, Alterable Storage Media.
- 2.2.3 The server-assisted slot machine or client station must support a command(s) that causes the server-assisted slot machine or client station to authenticate any software downloaded from the server. The server-assisted slot machine or client station must be disabled if the authentication is unsuccessful. This authentication must be transparent and must not interfere with the normal operations at the server-assisted slot machine or client station.
- 2.2.4 Each time a server-assisted slot machine or client station is powered up or rebooted and, in any event, on a random basis at least once every twenty-four hours, the server-assisted slot machine or client station must automatically authenticate the downloaded software by performing the authentication required by section 2.2.2 above. This automatic authentication must be transparent and must not interfere with the normal operations at the server-assisted slot machine or client station. The random authentication may be initiated by the server-assisted slot machine, client station or the slot machine server.
- 2.2.5 In the event that a server-assisted slot machine software authentication fails pursuant to the requirements of section 2.2.3 or 2.2.4 above, and a tilt mode is entered, the server-assisted slot machine must execute the following, if technically possible:
- a) Record the details of the tilt in a log, which must include at a minimum, the type of tilt, time, date, and slot machine event; and
 - b) Either automatically generate an alert notification of the tilt or, if the server-assisted slot machine is not capable of such alert notification, cause an appropriate tower light state pursuant to Electronic Gaming Equipment Minimum Technical Standards section 26, Tower Light.
 - c) If the server-assisted slot machine is capable and is connected to an approved computerized gaming management system, transmit a signal to the gaming management system indicating the type of tilt.
- 2.2.6 In the event that a server-based slot system software authentication fails pursuant to the requirements of section 2.2.3 or 2.2.4 above, and a tilt mode is entered, the slot machine server must execute the following:
- a) Record the details of the tilt in a log, which must include at a minimum, the type of tilt, time, date, and slot machine event; and
 - b) Either automatically generate an alert notification of the tilt or, if the client terminal is not capable of such alert notification, cause an appropriate tower light state pursuant to Electronic Gaming Equipment Minimum Technical Standards section 26, Tower Light; and

- c) If the server-based slot system is connected to an approved computerized gaming management system, transmit a signal to the gaming management system indicating the type of tilt.

2.2.7 Program media that contains critical software or is a vital component of the authentication process but cannot be interrogated (such as Smart cards) must have an alternative authentication method as accepted and approved by the Registrar.

2.3 Field Authentication of Software on the Server

2.3.1 Prior to the loading or installation of any software on a slot machine server, the new software will be subject to authentication by the AGCO. All critical software on the slot machine server must be capable of being authenticated by an independent device or software which, at a minimum, must authenticate each message digest of the designated software to ensure that it is an authentic copy of the approved software. The method of authentication must use an approved standard with at least 128 bits of resolution or an alternative authentication configuration determined by the Registrar to be equally or more secure.

2.3.2 The slot machine server must provide a secondary authentication method based upon a user seed input of at least thirty-two bits. The authentication method must return an authentication result of at least thirty-two bits corresponding to the critical software presently installed on the slot machine server.

2.3.3 The slot machine server must provide a secure interface port through which the software on the server may be authenticated and validated.

2.4 Field Authentication of Software on the Server-Assisted Slot Machine and Client Station

2.4.1 A server-assisted slot machine and client station must contain a method with which its software may be authenticated pursuant to Electronic Gaming Equipment Minimum Technical Standards section 12, Field Verification of Critical Software.

2.4.2 A server-assisted slot machine must contain a secure interface port through which its software can be authenticated.

2.4.3 Server-based slot systems must provide a secure interface port through which the software on the client station may be authenticated.

2.4.4 Server-based slot systems must provide for a secondary authentication method based on a user input seed of at least thirty-two bits. The authentication method must return an authentication result of at least thirty-two bits corresponding to the critical software presently installed on the client station.

3 Backup and Recovery

3.1 Data Backup

3.1.1 The slot machine server must be designed to protect the integrity of critical information in the event of a failure. Fault tolerant methods include, but are not limited to, mirroring data on two or more hard drives or having multiple hard drives in a RAID configuration. The method used must be capable of supporting daily backups and restoration. Any other type of redundancy scheme must be reviewed and approved by the Registrar.

3.2 Archive/Data Warehouse

3.2.1 Data may be transferred from a slot machine server to a data warehouse, provided that the interface for any request for information maintained in the data warehouse is:

- a) Based on a specific defined protocol or a specific set of defined commands that permit retrieval of information in response to an external request; and
- b) Capable of supplying the requested information while isolating the external request from the server-assisted slot machine game components, software and data.

3.3 Server-Based Server Backup

3.3.1 Each server-based slot system must have a secondary server available to immediately and automatically resume the primary server operation without loss of data in the event that software or hardware components of the primary server fail. In the event that the automatic resumption does not operate as expected, manual resumption is permitted.

3.3.2 In the event that the secondary server is unable to resume operation, it must be possible to reload the slot machine server from the last known good backup and fully recover the contents of that backup. The following information, at a minimum, is required to be recovered in the backup:

- a) Audit information;
- b) Security events;
- c) Configuration information for the slot machine server and client terminals;
- d) User permissions;
- e) All approved software; and
- f) All system databases.

3.3.3 The gaming site operators must submit to the Registrar for approval their disaster recovery plan, which details the plan to resume server-based gaming operations in the event the current server room becomes inoperable.

4 Software Download and Installation

4.1 Scheduling Software

- 4.1.1 A server-assisted or server-based slot system may contain or control scheduling software which instructs the slot machine server to download critical software or computer files to connected server-assisted slot machines or client stations, and to activate, modify or deactivate such programs, either on demand or at pre-established times and dates. The scheduling software must be installed only on the slot machine server in the computer server room, and must be approved by the Registrar prior to installation.
- 4.1.2 Scheduling software must include, at a minimum, reports of all pending, successful and unsuccessful events, including the user name, date, time, identification numbers of critical software and computer files successfully or unsuccessfully added, deleted, moved, activated or deactivated, and the status of each event.
- 4.1.3 Access to the scheduling software may be provided at terminals in secure restricted locations as approved by the Registrar, provided:
 - a) All communication between the terminal(s) and the scheduling software uses a secure channel.
 - b) The terminal(s) only allow authorized “execute only” access for the purposes of scheduling.
 - c) “read only” access to the scheduling software is provided to AGCO personnel authorized by the Registrar.
- 4.1.4 Any additions, deletions or changes to the scheduling software itself shall be performed in the presence of an AGCO representative designated by the Registrar.

4.2 Change Controls

- 4.2.1 At a minimum, on a daily basis and prior to any critical software being added to or removed from a server-assisted slot machine or client station, any configurable option changes or any activations or deactivations of a slot machine game on a server-assisted or server-based slot system, a complete set of slot machine game data must be successfully and accurately communicated to the slot machine server, a slot management system or another approved slot accounting system to include, but not be limited to, the following:
 - a) Error Logs, Electronic Gaming Equipment Minimum Technical Standards section 11, Error Conditions;
 - b) All applicable meters required by Electronic Gaming Equipment Minimum Technical Standards section 18, Meters;
 - c) Last Game Recall for client stations, Electronic Gaming Equipment Minimum Technical Standards section 17, Last Game Recall;
 - d) Cashless Transaction Logs, Electronic Gaming Equipment Minimum Technical Standards section 5, Cashless Wagering System.
- 4.2.2 Software must not be activated, deactivated, added to, modified or removed from a server-assisted slot machine or client station while an error or tilt condition, or handpay lockup exists on the server-assisted slot machine or client station, except as necessary to rectify the error or tilt condition.

- 4.2.3 Notwithstanding any slot machine game deemed to be or suspected as non-compliant with the AGCO Minimum Technical Standards, a slot machine game, once activated for play and offered on a server-assisted or server-based slot system, must be available at all times to all patrons under the same terms and conditions of play, and may not be permanently removed from play, until its actual payback achieves the minimum mandated percentage (equal or greater than 85% per requirement 20.1.2 of AGCO Electronic Gaming Equipment Minimum Technical Standards, Payback Percentage) at which time it may be scheduled for deactivation by the operator pursuant to 4.4.3 and made unavailable for play.

Slot machine games that have not achieved the minimum mandated percentage may be temporarily disabled or removed from play as part of normal operations but must be made available for play at a later date, no more than seven (7) days from the date they were temporarily disabled or removed from play, under the same terms and conditions on the original machine. The server-assisted slot machine or server-based server must retain meters for such games until they are permanently removed from play.

Any exception to this requirement will require approval by the Registrar on a case-by-case basis.

- 4.2.4 The removal of any software from a server-assisted slot machine, client station or slot machine server must in no way affect the requirement to maintain and store the logs of events related to that software and created pursuant to sections 7.2.1 and 7.2.2 below.
- 4.2.5 All configurable options in a slot machine game offered on a server-assisted or a server-based slot system that are governed by critical software must be configured prior to activation of the slot machine game. Game option settings are to comply with the applicable provisions of Electronic Gaming Equipment Minimum Technical Standards section 13, Game Options.

4.3 Slot Machine Requirements for Download and Installation

- 4.3.1 Whenever software is downloaded or configuration data is sent to a server-assisted slot machine or client terminal from the slot machine server, the server-assisted slot machine or client station must automatically:
- a) ensure that all software and data sent is or was completely and accurately received; and
 - b) detect the presence of corrupt or lost data packets and, as necessary, reject the transmission or prevent execution of the program.
- 4.3.2 Software downloaded to a server-assisted slot machine or client station must be initially stored in a separate area or partition of memory or hard disk space located in the server-assisted slot machine or client station, so that the downloaded software is segregated from the slot machine's operating software and cannot affect the current operation of the slot machine.

- 4.3.3 The downloaded software must be completely authenticated by the slot machine server prior to performing any operation on the software including, but not limited to, decrypting, extracting, uncompressing, and activating. The downloaded software must not be applied or made available for play until such time as the server-assisted slot machine or client station has met the conditions for changing the software pursuant to section 4.3.4 below.
- 4.3.4 Whether implemented manually or automatically, the server-assisted or server-based slot system must not permit any activation of gaming software, payable (payback/game theme) change or configuration changes to occur until the server-assisted slot machine or client station meets all of the following conditions:
- a) Be in idle mode with no game play, no credits, no handpay, no tilts or error conditions for at least four minutes prior to activation of gaming software, payable change or configuration changes;
 - b) During activation of any change such as new game or payable activation or configuration changes, the server-assisted slot machine or client station on which the game is offered must be disabled and rendered unplayable for the longer period of at least four minutes, or until the activation or implementation process is successfully completed;
 - c) While the server-assisted slot machine or client station is disabled for activation, the server-assisted slot machine or client station on which the game is offered must continuously display a conspicuous message stating that the game configuration is being changed. A patron, however, may have the option to bypass this message if he/she chooses to resume play prior to the end of the required time period; and
 - d) If the change in the active software is the direct result of a player request, the delay requirements of this technical standard are not applicable. However, the active software may not be changed if an error or tilt exists, or if a pending handpay remains on the server-assisted slot machine or client station.
- 4.3.5 Before a game is made available for patron play, one of the following conditions must be met:
- a) There is a clear change to the game display from the previously activated game where the patron can determine that there has been a change made to the game, e.g. a new theme, denomination, notification of the date/time of the last configuration, etc;
 - b) The payable is unavailable for play for a period of twenty four (24) hours; or
 - c) A sign or notification declaring that a change is to be made has been placed or displayed on the machine for a period of twenty four (24) hours before the change is made.
- 4.3.6 The change procedure described in section 4.3.4 above must also apply to an activated server-assisted slot machine or client station that offers multiple games.
- 4.3.7 Alarms required but not limited to Electronic Gaming Equipment Minimum Technical Standards sections 3.3.2, 11.1.2b), and 11.1.3c), Tilt Conditions, as applicable, must be able to be communicated to the gaming management system and/or slot machine server during any part of the download and activation process.
- 4.3.8 Any feature or setting of a slot machine game which is not approved for use must be disabled by:

- a) rendering such feature or setting unreachable in the server-assisted slot machine or client station through the game's critical software source code (also known as "commenting it out") by the program's logical control prior to its being compiled into machine-readable form; or
- b) disabling such feature or setting in the configurable options of the slot machine game's program through the use of a hardware device, secure password or other restricted technical procedure approved by the Registrar.

4.4 Operational Requirements for Download and Installation

- 4.4.1 Critical software must be approved for use in Ontario by the Registrar before it may be loaded on a slot machine server and/or installed on a server-assisted slot machine or client station.
- 4.4.2 Prior to a non-emergency installation, removal or implementation of any software, software change, software upgrade or configuration change to a slot machine server's operating system, or any hardware or networking addition, modification or replacement to a slot machine server, an operator must provide at least seventy-two hours advance written notice to the Registrar in accordance with the requirements of this section. Notwithstanding the foregoing, the Registrar may permit an operator to change or upgrade non-critical software files or directories or hardware governed by this subsection and specifically identified in the operator's approved internal controls, provided that written notice in accordance with the requirements of 4.4.5 shall be filed within twenty-four hours following the change.
- 4.4.3 Prior to a non-emergency installation or removal of any slot machine software, or a software change, software upgrade or configuration change to slot machine software on a slot machine server, server-assisted slot machine or client station, an operator shall provide at least forty-eight hours advance written notice to the Registrar in accordance with the requirements of 4.4.5.
- 4.4.4 Prior to an emergency installation, implementation or removal of any software, or a software change, software upgrade or configuration change to any software on a slot machine server, or any hardware or networking addition, modification or replacement to a slot machine server that is required as a result of a software or equipment malfunction, an operator must immediately notify the Registrar, and must provide the Registrar written notice in accordance with the requirements of 4.4.5 below within twenty-four hours following the completion of the change.
- 4.4.5 Any written notice filed by an operator in accordance with sections 4.4.2, 4.4.3 or 4.4.4 must include, without limitation, the following:
 - a) A description of the reasons for the proposed modification;
 - b) A list of the computer components and programs or versions to be modified or replaced;
 - c) A description of any screens, menus, reports, operating processes, configurable options or settings that will be affected;
 - d) The method to be used to complete the proposed modification;
 - e) The date the proposed modification will be installed and the estimated time for completion;
 - f) The name, title, and employer of the person or persons who will install the proposed modification; provided however, that the person providing the notification shall not be among the persons installing the modification;

- g) A diagrammatic representation of any proposed hardware design change; and
 - h) Representations as to whether user and operator manuals will need to be updated to reflect changes in policies or procedures resulting from the proposed modification, and whether such updates have been made, and if not, when the changes will be implemented.
- 4.4.6 Subject to any testing required by the Registrar upon receipt of the notification required by section 4.4.5 above, any modifications to a slot machine server or the software thereon will, subject to the Registrar's discretion, be installed in the presence of an AGCO representative.
- 4.4.7 An operator must submit or make available electronically, pursuant to section 4.1 Scheduling Software, the following scheduling software information to the Registrar:
- a) A list of each proposed schedule, prior to its implementation; and
 - b) A notice of each change in a previously submitted schedule and any other changes, prior to implementation of the change.

5 Error Conditions

- 5.1.1 The slot machine server must immediately notify the operator of any malfunctioning element upon the occurrence of any communication failure, and must report the results of a self-monitoring process that is run, at least once each gaming day, on each of the system's critical interface elements (such as central hosts, network devices, firewalls) and notify the operator of any malfunctioning element.
- 5.1.2 Pursuant to Electronic Gaming Equipment Minimum Technical Standards section 14.2.4, where an unrecoverable memory corruption must result in a RAM error that requires a full RAM clear, the RAM clear event must be performed in a secure manner after authorization from a representative of the Registrar, whether the RAM clear is performed from the slot machine server, the server-assisted slot machine or client station.
- 5.1.3 A server-based game must be rendered unplayable if communication from the server is lost. The client station must provide a means, such as a hand pay or the issuance of a payout voucher, for patrons to cash out credits indicated on the client station at the time the communications was lost. If a payout voucher is issued, the system must ensure proper reporting and accounting of the voucher.

6 Meters

- 6.1.1 Server-assisted slot machines must record, store and maintain the meters required in Electronic Gaming Equipment Minimum Technical Standards section 18, Meters. The server-assisted slot machine must also record all such meters for each individual slot machine game (each specific payable) that is activated on that slot machine.
- 6.1.2 The required meter information for server-assisted slot machines (from 6.1.1) must be stored and maintained on either the slot machine server or the connected slot monitoring/accounting system at a minimum on a daily basis, on demand and at the time a cash box is removed.
- 6.1.3 Server portions of system-based slot systems must record, store and maintain meters required in Electronic Gaming Equipment Minimum Technical Standards section 18, Meters. The server portion of system-based slot systems must also record all such meters for each individual slot machine game (each specific payable that is activated on each individual client station, as well as for the server-based game in its entirety. The server must be able to send this meter information to a slot monitoring/accounting system, if the server-based slot system is not capable of generating the necessary accounting reports.
- 6.1.4 Client stations must be able to display on demand the required meter information (from 6.1.3) that corresponds to the play associated with the particular client station.

7 Reports and Logs

The slot machine server report requirements of this section may be satisfied by the slot machine server and/or the slot accounting/monitoring system.

7.1 Server Requirements for Reports and Audit Logs

- 7.1.1 Logical access to the slot machine server shall be logged on the server and on a secondary logging device which resides outside the server room and is not accessible to the individual accessing the server room. This information is not required to be logged on the secondary logging device if the information has been rendered unalterable, through a means approved by the Registrar, on the server. Logged data shall include time and date of the access and the identification of the accessing individual(s). The resulting logs shall be retained for a minimum of ninety days. AGCO representatives must have free and unfettered access to all logs created pursuant to this standard.
- 7.1.2 A slot machine server must create a log entry, at a minimum, every time any critical software component is added, removed or altered in the slot machine server, which must contain:
- a) The date and time of the action;
 - b) Identification of the software affected, both removed and installed;
 - c) The names and unique identification (e.g. registration ID) of the individuals performing the modification including configuration changes per section 1.4.4f);
 - d) The reason for the modification and any pertinent validation information.
- 7.1.3 The slot machine server must create a log entry whenever any change is made to software in a server-assisted slot machine or client station, including but not limited to software programs, graphics, sound information and configuration changes. This log entry must contain the date and time of the event, an identification of the software affected, the name of the individual performing the modification, and any pertinent software identification information. The log entries must be retained on the slot machine server for a minimum of ninety days; provided that logged events older than ninety days may be archived in a manner and secure location approved by the Registrar.
- 7.1.4 The slot machine server must be capable of generating a record detailing any software modification to the slot machine server, or, if not capable of generating such a record, an alternative method of record keeping must be performed as approved by the Registrar. In the event the Registrar determines that testing is required after the modification, the Registrar will establish the terms and conditions of the test.
- 7.1.5 The slot machine server must generate daily monitoring logs with the date and time of:
- a) User access;
 - b) Security incidents; and
 - c) Any other logged events which reasonably indicate that the system is not operating as expected, e.g. memory corruption, authentication failure.

The slot machine server must be capable of immediately notifying the appropriate departments of such security incidents and events. The daily logs must include all associated information available from the system to readily identify the nature of the security incident or other event.

7.1.6 The slot machine server must be capable of maintaining the logs on the slot machine server and the other logging device referenced in sections 7.1.1, 7.1.2, 7.1.3 and 7.1.4 above, for a minimum of ninety days. All logs must be archived for a period as outlined by the Internal Controls of the operator, in a manner and secure location approved by the Registrar. All log files must be protected against modification and loss by either:

- a) creating the log files by a “write once, read many” (WORM) technology that must not be susceptible to change; or
- b) utilizing access controls over such logs and procedures to ensure that information is not written over or deleted which may include, but not be limited to, controls restricting system administrator level access to a minimum of two individuals using split passwords, dual keys or any other suitable method as approved by the Registrar. The joint but not separate access may be achieved with the two individuals consisting of a representative of the manufacturer or operator and an authorized AGCO representative.

7.1.7 The slot machine server must be capable of retaining a record and generating a report pursuant to section 7.2.1 and 7.2.2 below of all titles of all active slot machine games offered on all server-assisted slot machines or client stations, and all changes made to any of the slot machine games, for each twenty-four hour period the slot machine games are in operation.

7.2 Server-Assisted Slot Machine and Client Station Requirements for Reports and Audit Logs:

7.2.1 Whenever any change is made to software in a server-assisted slot machine, including but not limited to software programs, graphics or sound information, a log entry must be made on the server-assisted slot machine which must contain the date and time of the event and an identification of the software affected. The logs must be capable of being retained on the server-assisted slot machine for a minimum of 100 logged events.

7.2.2 Whenever any change is made to software in a client station, including but not limited to software programs, graphics or sound information, a log entry must be made which must contain the date and time of the event and an identification of the software affected. This log entry must be made either on the client station, or on a secondary logging device which resides outside the server room and is not accessible to the individual making the program modification. This information is not required to be logged on the secondary logging device if the information has been rendered unalterable, through a means approved by the Registrar, on the server.

7.3 General Requirements for Reports and Audit Logs:

- 7.3.1 Gaming equipment reports must be generated for each server-assisted slot machine and client station pursuant to the criteria in Electronic Gaming Equipment Minimum Technical Standards sections 5.2 and 5.3, Cashless Wagering System. For server-assisted systems, these reports may be generated by the connected slot accounting system. Additionally, the following reports must be available to the representative of the Registrar:
- a) A report by game and payable for all paytables that have not achieved the minimum payback percentage; and
 - b) An audit report that details the results of tests performed on gaming devices before being available for play.
- 7.3.2 Each report contained herein must include the report title and date and time the report was generated. The slot machine server must be able to generate reports with all or any subset of the following information as it pertains to the system:
- a) User access rights by user and by role;
 - b) System configurations;
 - c) List of all active gaming devices;
 - d) List of all deactivated gaming devices;
 - e) All software installed on the slot machine server;
 - f) All games and paytables installed on the slot machine server;
 - g) All games and paytables active on the gaming floor with location and gaming device information;
 - h) All game and payable changes to be reported in daily, weekly and monthly periods; and
 - i) A report of all progressive jackpots listing the participating games.
- 7.3.3 All information required to be logged pursuant to this section must be available on demand in a daily, weekly and monthly report format. The AGCO may, at its discretion, require custom reports from the required logged information. Each log report required herein must include the report title and the date and time the report is generated. Where applicable, audit logs will include the source and destination IP addresses, port numbers and MAC addresses. At a minimum, the following log reports must be available and include the information in the referenced requirement:
- a) A firewall log report pursuant to section 1.3.6b) above;
 - b) A software integrity log report pursuant to section 2.1.4b) above;
 - c) A slot machine server log report pursuant to sections 1.4.4g), 7.1.2, 7.1.4 and 7.1.5 above;
 - d) A server-assisted slot machine and client station log report pursuant to sections 7.1.3 and 7.2.1 above;
 - e) A daily monitoring log report pursuant to section 7.1.5 above;
 - f) A scheduling log report pursuant to sections 4.1.2 and 7.3.2c) above;
 - g) A server-assisted log report pursuant to section 7.1.7 above;
 - h) A server-based log report pursuant to section 7.1.7 above; and
 - i) Software authentication log reports pursuant to sections 2.2.5 and 2.2.6 above
- 7.3.4 Progressive jackpot reconciliation reports must be available on a weekly basis and must include, by progressive jackpot level, the following:

- a) The coin in meter amount for each participating gaming device;
- b) The total of the coin in meter amounts;
- c) The progressive rate; and
- d) The current progressive amount.

8 Remote Access

8.1 Remote Access to Server-Assisted or Server-Based Slot Systems

- 8.1.1 Remote access is defined as any access to the system that does not comply with section 1.3.5. The security of any remote access method and associated procedures will be evaluated by AGCO prior to approval. Any authorized remote access must authenticate all computer systems based on the authorized settings of the slot machine server or firewall application that establishes a connection with the slot machine server.
- 8.1.2 Remote access to a server-assisted or server-based slot system may only be conducted with the server portion of the system.
- 8.1.3 A server-assisted or server-based system may only be accessed using a method that securely links the system to the remote server requesting access. This secure link must uniquely identify the remote server requesting access as an entity authorized to conduct remote communications with the gaming device.
- 8.1.4 A server-assisted or server-based system must provide a hardware or software mechanism that defaults to and remains in a disconnected state unless specifically set to allow communications as a result of a command issued by the slot machine server. Additionally, upon completion of the communications, the device must sever the connection between the slot machine server and the remote access terminal.
- 8.1.5 A server-based or server-supported system must log each remote access on the server and on the secondary logging device, if used to comply with these standards. The log must include time and date of the access and a list of programs transferred or changed.
- 8.1.6 Any remote access to the slot machine server, whether or not write capability is permitted, must be initiated by the operator and only granted to either the operator or the registered supplier from their respective place of business provided:
- a) Access is user ID and password protected;
 - b) The system automatically monitors and records the log-on name, time and date the connection was made, duration of the connection, and activity while logged-in, including the specific areas accessed and changes made;
 - c) Both the operator and the supplier, if the case may be, submit a monthly log to the AGCO documenting, for each remote access, the start date and time, end date and time, reason for access, and person making access;
 - d) Operators wishing to utilize on-going remote capability must submit a written request with specific reasons and receive written approval for such access from the Registrar;
 - e) No unauthorized remote user administration functionality is permitted (such as adding users, changing permissions, etc.)
 - f) No unauthorized access to the system is permitted, including but not limited to, databases, the operating system, scheduling software, etc; and
 - g) The secondary logging device, if used to comply with these standards, is operational and is communicating with the system.

9 Forensic Capabilities

- 9.1.1 It must be possible to perform a forensic analysis of any anomaly that occurs which may include viewing the data at the slot machine server and being able to place the data onto a duplicate device for the examination without shutting down or compromising the integrity of the production server.

10 Other Requirements

- 10.1.1 A gaming-related supplier that provides software for a server-assisted slot machine or client station must submit for review and approval by the Registrar internal controls and any subsequent amendments for the creation, application and use of digital signatures as applicable in connection with any software for a server-assisted slot machine or client station, including, but not limited to, the procedures for the security of the private key and the types of digital signatures in question.
- 10.1.2 A gaming-related supplier must make available upon demand to the Registrar a list of the employees or other persons who have access to and can authorize the use of the private key that creates digital signatures for that software. The gaming-related supplier must update the list within seventy-two hours of each addition or other change.
- 10.1.3 All aspects of a slot machine server, including all hardware and software, are subject to testing and approval by the Registrar prior to the installation and use of the slot machine server by the operator and, after installation, prior to any changes thereto.

11 Compliance with AGCO's Electronic Gaming Equipment Minimum Technical Standards

- 11.1.1 Server-assisted and server-based slot systems must also comply with the AGCO's Electronic Gaming Equipment Minimum Technical Standards as applicable, unless stated otherwise in this document.
- 11.1.2 The gaming operators must comply with the requirements listed in the AGCO's directive, "Requirements for Changes to Gaming Equipment and Gaming Management System" issued by the AGCO for installation, changes and removal of progressive games.

Glossary

Activated Game: A slot machine game that is available for play at a server-assisted slot machine or client station.

Alterable Storage Media Device: Any electronic storage media whose contents can be modified through the use of gaming equipment circuitry or programming. This does not include RAM or media that has its write functionality disabled.

Authentication Software: A program which uses an authentication algorithm or other standard method of authentication with:

- a) At least 128 bits of resolution (e.g. MD5, SHA-1) or a bit-by-bit comparison that the Registrar has approved for use in authenticating the software; or
- b) An alternative authentication configuration determined by the Registrar to be equally or more secure as (a) above, such determination to be made prior to the approval of a server-assisted slot system.

Client Station: Gaming equipment which is connected to and administered by a server-based slot system and is the public interface part of a server-based slot system that cannot operate independently from the system.

Configurable Options: Settable options required to ensure the integrity, security and accounting capability of the game.

Critical Software: Any gaming-related software that:

- a) is integral to the operation of a game; or
- b) is used to control game functions, game outcome, payout, security or accounting functions.

Data Warehouse: A device that receives and stores data from a slot machine server and is physically and logically segregated from that slot machine server.

Deactivated Game: A slot machine game that is no longer available for play on the server-assisted slot machine or client station due to changes in slot machine configurations.

Digital Certificate: An electronic identification credential attached to transmitted data that:

- a) is initially created and subsequently authenticated in a manner and frequency approved by the Registrar; and
- b) uniquely authenticates the identity of the sender in a manner approved by the Registrar, using a generally accepted method for secure computing.

Digital Signature: An encrypted message digest that is initially created and subsequently authenticated in a manner and frequency approved by the Registrar and is used to authenticate the origin of the software program, file or data in a manner approved by the Registrar.

Message Digest: An electronic signature created, for example, with the MD5 or SHA1 algorithm, attached to a software program, file or data, that is used to ensure that the contents of the software program, file or data were not changed in any manner whatsoever after the message digest was created.

Play: All gaming events that may be initiated by the making of a specific wager. A play includes the making of a wager, the activation of the gaming equipment game by the patron and an indication to the patron of the outcome of the wager including, if an award is won, the payment of the award.

Random number generator: Hardware and/or software used to generate numbers which exhibit randomness.

Server-Assisted Slot Machine: Gaming equipment connected to and administered by a server-assisted slot system and is the public interface part of a server-assisted slot system. A server-assisted slot machine must be able to operate independently from the server-assisted slot system.

Server-Assisted Slot System: A system comprised of one or more server-assisted slot machines connected to a slot machine server and an associated computer network which provides access to approved slot machine games and other related software from the slot machine server to the server-assisted slot machine. In a server-assisted slot system, the game outcome is determined by the server-assisted slot machine. Any design that deviates from this concept will be considered on a case-by-case basis by the Registrar.

Server-Based Slot System: A system comprised of one or more client stations connected to a slot machine server and an associated computer network which provides access to approved slot machine games and other related software from the slot machine server to the client stations. In a server-based slot system, the game outcome is determined by the server. Any design that deviates from this concept will be considered on a case-by-case basis by the Registrar.

Slot Machine Server: A dedicated computer system that receives and stores approved server-assisted or server-based slot system software, including game software, and authenticates the critical software. The slot machine server uploads and communicates with the connected server-assisted slot machines and client stations. A slot machine server is also used to effect changes in the configuration of connected server-assisted slot machines or client stations. Nothing herein shall preclude a server-based or server-assisted slot system design that utilizes more than one slot machine server. All slot machine servers are subject to approval by the Registrar.

Slot Machine Server Room: A physically separated, secured location containing the slot machine server. The slot machine server room is to be located within Ontario and, with prior approval from the Registrar, may be located within a secure area that contains other computer systems.

Tilt: A programmed error or alert state for a gaming device. A tilt condition has occurred when the device detects an internal error, malfunction, attempted cheating, or a state that does or may affect the gaming device operating condition and the tilt condition disallows further play until the tilt is resolved unless otherwise authorized by the Registrar which may include such tilt

conditions as low printer paper supply, bill validator stacker full or such other tilt conditions as approved by the Registrar.