INTEGRITY CERTIFICATION REQUIREMENTS: **CENTRAL SYSTEMS FOR SLOT MACHINES**

Saskatchewan Liquor and Gaming Authority

June 2005

Introduction

The Saskatchewan Liquor and Gaming Authority (SLGA) is responsible for the regulation of gaming in Saskatchewan as mandated under *The Alcohol and Gaming Regulation Act, 1997*.

SLGA may according to *The Alcohol and Gaming Regulation Act, 1997*, set the terms and conditions of gaming supplier certificates of registration. In the event that SLGA issues a gaming supplier certificate of registration to you, that certificate of registration will include a term that you shall at all times comply with all applicable Gaming Integrity Standards established by SLGA from time to time.

This document outlines the technical gaming integrity standards for the central systems required to operate slot machines in casinos.

Background

These standards were developed in consultation with Saskatchewan Gaming Corporation, Saskatchewan Indian Gaming Authority, Western Canada Lottery Corporation, and Saskatchewan Liquor and Gaming Authority. Additionally, documents on central systems were consulted as: Gaming Laboratories Incorporated (Standard Series 16,18,20,21, Version 1.3, November 10th, 2000); Nevada Gaming Control Board (Technical Standards for Electronic Gaming Devices, January 15, 1999), West Virginia (limited Video Lottery Act), and discussions with other Canadian jurisdictions.

Purpose

These standards are intended to provide regulatory guidance to manufacturers, suppliers and gaming operators about acceptable technical gaming integrity requirements in Saskatchewan. Where practices amongst operators may differ from acceptable standards, SLGA as the regulator will review to determine acceptable practices.

These standards provide the basis for consistent public policy. They are founded on objectives that meet the test for: fairness, accountability, security, honesty, reliability, and safety.

General

1.1 Ownership and Control of Technical Gaming Integrity Document

The ownership and control of this document and all subsequent amendments rest with SLGA.

1.1.1 Document Revision

Technological change in the industry may require SLGA to issue corresponding amendments and changes to previously approved standards. Reasonable notice will be given to all manufacturers, supplies, testing laboratories and operators, for implementation.

1.02 Parameters of Document

This document is intended to outline those standards that apply to central systems for slot machines, covering: hardware, software and data base requirements, systems communications, reporting, security features, ticket validation, progressive jackpot systems, bonus systems, cashless systems, and promotional systems.

SLGA recognizes that site operators may potentially have different systems providing specific features to the casino interlinked to operate transparently as one large central system for a casino. This document takes this into account and stresses that these standards shall be interpreted in either of two ways:

a) The central system can be viewed as an aggregate assembly of multiple systems interlinked to operate transparently as one system, or;
b) Each component of the central system can be viewed separately but the assumption will be made that all components shall operate as an aggregate assembly to form one transparent system.

1.03 Technology

SLGA recognizes that gaming technology changes. New technology will be evaluated, as required, and the standards amended accordingly as per section 1.1.1 of this document.

1.04 Regulatory Requirements

Manuals

Operation manuals and service manuals must be expressed in broad terms that are directly relevant to the complete gaming system. At a minimum, manufacturers must provide the following information for review to both SLGA Compliance Branch and an independent testing laboratory approved by SLGA before any system is approved for use in Saskatchewan:

a) Operational manuals associated with the applicable system;
b) Training manuals;
c) Technical Service manuals which:
   - Accurately depict the central system for which the manual is intended to cover;
   - Provide adequate detail and be clear in their wording and diagrams to support use by slot technicians and other maintenance personnel;
   - Include amaintenance schedules outlining the elements of the central system that require maintenance and the frequency at which that maintenance should be carried out;
   - Include a maintenance checklist that enable appropriate staff to make a record of the work performed and the results of the inspection; and
   - Include a complete list and samples of available reports that can be generated by the system.

d) Technical documentation that includes: wiring diagrams, structure diagrams, flow charts, schematics, etc. relevant to the proprietary devices specific to the gaming system. Circuit schematic diagrams must accurately depict the central system for which the diagrams are intended to cover. They must also provide adequate detail and be sufficiently clear in their wording and diagrams to enable qualified technical staff to perform an evaluation on the design of the component, and be professionally drafted in order to satisfy the above requirements; and

e) Complete documentation for programming patches, fixes and any upgrades made to the system.

2.00 Interface Devices

2.01 Interface Device Hardware and Software Requirements

Each electronic gaming device installed in the casino must have an interface device installed for communication between the electronic gaming device and the central system. The interface shall not interfere with the communication of any other devices attached/sharing the communication system either through normal communication or if a malfunction occurs with the interface device.

2.02 Certified

The interface device shall be CSA or UL certified for use in Canada.

2.03 Battery Backup Requirements

The interface device must retain the required information after a power loss for a period of no less than 12 months. If this data is stored in volatile RAM, a battery backup must be installed within the interface device.

2.04 Technical Diagnostics.

The interface shall have the capability of visually indicating the status of communications to and (TX/Rx host) from the central system and to and from (Tx/Rx EGD). This can be utilized by LED's, seven segment displays, or any other acceptable means.

2.05 Metering Requirements

If not directly communicating electronic gaming device meters, the interface device must maintain separate electronic meters of meters of sufficient length to preclude loss of information from rollover as provided for in the connected electronic gaming device. These electronic meters should be capable of being reviewed on demand, at the interface device level via an authorized access method, see also '**Section 8 'Meters.**'

2.06 Information Buffering and Integrity Checking

If unable to communicate the required information to the central system, the interface device must provide a means to preserve all mandatory meter and significant event information until at such time as it can be communicated to the central system, see also '**7.01 Event Format**' and **Section 8 'Meters.'** Electronic gaming device operation may continue until

critical data will be overwritten and lost. There must be a method to check for corruption of the above data storage locations.

2.07-2.10 Reserved for Amendments

2.11 Address Requirements

The interface device must allow for the association of a unique identification number to be used in conjunction with an electronic gaming device file on the central system. This identification number will be used by the central system to track all mandatory information of the associated electronic gaming device. Additionally, the central system should not allow for duplicate "active" electronic gaming device file entries of this identification number.

2.12 Configuration Access Requirements

The interface device setup/configuration menu(s) must not be available unless using an authorized access method.

2.13 Clearing Meters

An interface device should not have a mechanism whereby an unauthorized user can cause the loss of stored accounting meter information.

3.00 System Hardware Requirements

3.01 Hardware and Player Safety

Individual hardware may be approved separately providing the hardware has met the outlined standards described AND the manufacturer provides documentation to SLGA describing the purpose or reason for testing equipment separately from the central system.

3.02 Reserved for Amendments

3.03 Front End Controller and Data Collector Requirements

A central system may possess front end processors that gather and relay all data from the connected Data Collectors to the associated database(s). The data collectors, in turn, collect all data from connected electronic gaming devices. Communication between components must be via an approved method and at minimum conform to the communication protocol requirements stated in this document.

3.04 Server and Database Requirements

A central system will possess a server(s), networked system or distributed systems that direct overall operation and an associated database(s) that stores all entered and collected system information.

3.05 System Clock

A central system must maintain an internal clock that reflects the current time (24hr format) and date that shall be used to provide for the following:

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of all logged configuration changes.

3.06 Synchronization Feature

If multiple clocks are supported, the central system shall have a facility whereby it is able to update all clocks in the central system components. This includes clocking in: cashless, bonus, progressive and promotional systems. All internal clocks shall be synchronized by the central system.

4.00 Work Station Requirements

4.01 Jackpot/Fill Functionality

A central system must have an application that captures and processes every hand pay message from each electronic gaming device. Hand pay messages must be created for single wins (jackpots), progressive jackpots and accumulated credit cash outs (canceled credits), which result in hand pays. A fill (deposit of a predetermined, or otherwise properly authorized, token amount in an electronic gaming device's hopper) is normally initiated from a hopper empty message while a credit (removal of excess tokens from an electronic gaming device) is normally user initiated. An allowable exception to fill initiation would be where the system provides preventative or maintenance fill functionality, in which the transaction may be initiated by the system or an authorized user. Once captured by this application, there must be adequate access controls to allow for authorization, alteration, or deletion of any of the values prior to payment or execution.

4.02 Jackpot/Fill Slip Information

The following information is required for all slips generated with some/all fields to be completed by the central system:

a) Alphanumeric slip identifier;
b) Date and time (shift if required) ;
c) Electronic gaming device number;
d) Denomination;
e) Amount of fill;
f) Amounts of jackpot, accumulated credit, and additional pay;
g) Amount to patron;
h) Total coins played and game outcome of award;
i) Soft meter readings; and
j) Relevant signatures as required by SLGA.

The above information may vary dependent upon internal controls and may be subject to change.

4.03 Surveillance/Security Functionality

A central system shall provide an interrogation program that enables on-line comprehensive searching of the significant event log for the present and for the previous 14 days (at minimum) through archived data or restoration from backup where maintaining such data on a live database is deemed inappropriate. The interrogation program shall have the ability to perform a search based at least on the following:

a) Date and time range;
b) Unique interface device/electronic gaming device identification number; and

c) Significant event number(s).

5.00 Database Requirements

5.01 Management Functionality

A central system must have a master "electronic gaming device file" which is a database of every gaming device in operation, including at minimum the following information for each entry. If the central system retrieves any of these parameters directly from the electronic gaming device, sufficient controls must be in place to ensure accuracy of the information.

Additionally, the central system must accommodate the use of redemption units for use by track fills.

5.02 Parameters

The central system shall maintain the following information for gaming equipment associated with the central system:

a) Unique serial number of the electronic gaming device;
b) Electronic gaming device identification number as assigned by the casino;
c) Location;
d) Device description;
e) Game name or theme; and
f) Configuration;
    i. Denomination;
    ii. Software version/ control program(s) within gaming device;
    iii. Theoretical hold of the gaming device; and
    iv. Progressive status.

5.03 Database Access

The central system shall have no built-in facility whereby a casino user/operator can bypass system auditing to modify the database directly. Casino operators will maintain secure access control. All information related to files, internal and external transactions, terminals and programs must be protected to prevent unauthorized access, modification or destruction of data. See **Section 10.00 'Security Requirements'** for further database information.

5.04 Player Tracking

At no time shall the database be designed to record information that may breach The *Personal Information Protection and Electronic Documents Act*.

5.05 Modification of Patron Information

Only an authorized, logged employee shall change player information. Security of this information (including patron PIN codes or equivalent patron identification) must be guaranteed at all times.

5.06 Balance Adjustments

Any adjustment to an account balance outside of the normal methodology would require a supervisor's approval with all changes being logged and/or reported indicating who, what, when, and the item value before and after the change, with the reason.

5.07 Parameters

The central system shall maintain the following information for player tracking associated with the central system.

a. Name;
b. Mailing address;
c. Postal code;
d. Phone number and or fax number;
e. E-mail address (optional);
f. Player loyalty information (e.g. games played, number of days active, time on device, etc…); and
g. Game play patterns.

However, at no time shall the database track information that may breach legislated privacy laws in accordance to the *Criminal Code of Canada* and The *Personal Information Protection and Electronic Documents Act*.

5.08 Accounting Functionality

A central system must have an application that allows controlled access to all accounting (financial) information. This application shall be able to create all mandatory reports in **Section 9.01 'Reporting Requirements,**' as well as all required internal control reports.

6.00 Communication

6.01 Due Diligence

It is the responsibility of the manufacturer to ensure that the central system be designed to be as impervious to communications. It is up to the manufacturer of the central system to ensure that the system is tolerant of:

- "noise" such as "common mode" noise;
- AC noise;
- Signal attenuation and distortion;
- Signal termination;
- Ground loops;
- Shorting of any pair in communication wiring; and
- Open termination.

.

6.02 General Statement Regarding Communication

A central system must support a defined communication protocol(s) that provides for the following:

a) All critical data communication shall be protocol based and/or incorporate an error detection and correction scheme to ensure an accuracy of data received; and

b) All critical data communication that may affect revenue and is unsecured either in transmission or implementation shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication.

6.03 Error Recovery

The following conditions apply to error recovery:

a) The communications protocol must cater for recovery of messages when they are received in error or not received at all;

b) There must be positive acknowledgment of all valid data messages received. Note that this requirement implies two (2) way communications are mandatory;

c) Where multiple messages may have been sent it must be clear which messages have been positively acknowledged; and

d) There must be a method of automatic repeat request (ARQ) of messages received in error. Implementations may include negative acknowledgment (NAK) of messages received in error or time-out.

6.04 Hierarchy

a) For informational purposes, the manufacture shall provide all relevant protocol specifications employed by the central system;

6.05 Bi-Directional Requirements

Significant emphasis shall be placed on the integrity of the communication system for cashless gaming. With the requirement of "two-way communication" where credits or awards are transferred bi-directionally from the central system and the gaming device, the security of the system is paramount. Slot central systems will be held to the strictest and highest standards to ensure that:

a) The physical network is designed to provide exceptional stability and limited communication errors;

b) The system is stable and capable of overcoming and adjusting for communication errors in a thorough, secure and precise manner;

c) Information is duly protected with the most secure forms of protection via encryption, segregation of information, firewalls, passwords, personal identification numbers and any other methods known and unknown that may facilitate the level of security mandated by SLGA.

6.06 Encryption

For "Non-Cashless" systems, the following is preferred, but not mandatory. For "Cashless System," the following is MANDATORY

Security messages that traverse data communications lines must be encrypted using the best known form of encryption available at the time. The intent is that communications be demonstrably secure against crypto-analytic attacks.

At a minimum the following data must be transmitted in encrypted format to/from the central system:

a) Signature seeds (algorithm coefficients);
b) Signature results;
c) Encryption keys, where the implementation chosen requires transmission of keys;

d) Software uploads and downloads of any security related software (e.g. signature, RNG, game result determination, payout software); and
e) Other security related information.

See '10.00 SECURITY REQUIREMENTS' for further details.

6.07-6.10 Reserved for Amendments

6.11 System Functionality

The central system must have the ability to perform the following:
a) The ability to enable/disable gaming device;
b) The ability to retrieve a "snap shot" of information as it pertains to financial and games played on a specific gaming device; and
c) The ability to retrieve security data from a specific gaming device;
The optional ability to solicit an internal "self test" from an individual gaming device or group of devices which will report the state of internal components.

6.12 Wireless Technology

6.12.1 Non-critical applications

The use of wireless technology is acceptable for the purposes of building efficiency and cost savings into areas where no critical information is being transmitted or received. Areas of inclusion are:
i) Any situation where the signal is used to trigger an alarm, noise or sound used to inform the public of a prize won; and
ii) Update promotional messaging or other information.

6.12.2 Critical applications

Wireless technology is not allowed for use to transmit or receive any information that pertains to credits, personal identification number (PIN), player tracking, TITO, cashless gaming, or related functions. At this time, SLGA deems wireless technology to have inadequate security measures to prevent fraudulent, illegal or mischievous activity. When testing evidence demonstrates that the technology is secure, SLGA will review for inclusion as an acceptable standard.

6.13 Network Topologies

Network topologies do not require approval as long as the integrity of the central system is not compromised.

7.00 Events

7.01 Event Format

Events generated by or occurring at an electronic gaming device are sent via the interface device to the central system utilizing an approved communication protocol. Each event must be stored in a database(s) which includes the following:
a) Date and time which the event occurred;
b) Identity of the electronic gaming device that generated the event;

c) A unique code that defines the event; and
d) A brief text that describes the event.

7.02 Standard Events

The following standard events must be collected from the electronic gaming device and transmitted to the system for storage:

a) Power resets or power failure;
b) Hand pay conditions (amount needs to be sent to the system);
    i. electronic gaming device jackpot (an award in excess of the single win limit of the electronic gaming device);
    ii. Cancelled credit hand pay; and
    iii. Progressive jackpot (As per jackpot above.)
c) Transaction information (see other derivatives of "systems' included in this document for further details.) includes:
    i. Casino name;
    ii. Machine number;
    iii. Date and time (24hr format);
    iv. Alpha and numeric dollar amount of the ticket; and
    v. Ticket sequence number;
d) Coin or Token-In errors including:
    i. Coin or token jams; and
    ii. Reverse coins or tokens-in.
e) Bill (Item) Acceptor Errors including:
    i. Stacker Full (if supported); and
    ii. Bill (Note) jam.
f) Electronic gaming device low RAM battery error;
g) Reel spin errors (if applicable with individual reel number identified);
h) Coin or token-out errors; and
i) Hopper jams;) hopper runaways or extra coins paid out;
j) Hopper empties (must be sent as a unique message); and
k) Printer errors (if printer supported).

7.03 Priority Events

The following priority events must be conveyed to the central system in a timely manner:

a) Loss of communication with interface device;
b) Loss of communication with electronic gaming device;
c) Memory corruption of the interface device;
d) RAM corruption of the electronic gaming device;
e) Door openings (any external door on the electronic gaming device);
f) "Power off" door openings; and
g) Failed verification attempts (if verifications are supported by central system).

8.00 Meters

8.01 Information

Metering information is generated on an electronic gaming device and collected by the interface device and sent to the central system via a communication protocol. This

information may be either read directly from the electronic gaming device or relayed using a delta function. As well, the central system shall be able to compensate for "meter wrapping" and use a "meter recovery" technique to prevent data loss or corruption caused by "meter wrapping."

8.02 Required Meters

The following (minimum) metering information must be communicated from the electronic gaming device:

a) Total In (credits-in);
b) Total Out (credits-out);
c) Amount Wagered;
d) Amount Won;
e) Drop Meter;
f) Handpays (cancel credit);
g) Bills In (total monetary value of all bills accepted);
h) Items In (total value of all items accepted);
i) Individual Bill Meters (total number of each bill accepted per denomination);
j) Games Played (strokes);
k) Cabinet Door (instance meter which may be based on central system count of this event); and
l) Drop Door(s) (instance meter which may be based on central system count of this event).

NOTE: Please refer to the SLGA **SLOT MACHINE INTEGRITY STANDARDS, Section 4.56 'Electronic Accounting'** and **Section 3.68 'Machine Metering of Bill Acceptor Events'** for the electronic accounting meters that are to be maintained by the electronic gaming device. While these electronic accounting meters should be communicated directly from the electronic gaming device to the central system, it is acceptable to use secondary central system calculations where appropriate.

9.00 Reporting

9.01 Reporting Requirements

Significant event and metering information is stored on the central system in a database and accounting reports are subsequently generated by querying the stored information. The central system must have built in functions to permit the following: exportation data, investigation of anomalies, archiving of data, restoration of data, and ability to allow users to develop ad-hoc reports.

9.02 Required Reports

Reports at minimum will consist of the following:

a) Net win report for each electronic gaming device;
b) Monthly electronic gaming device revenue summary;
c) Drop comparison reports for each medium dropped (examples = coins, bills) with variances for each medium;
d) Metered vs. actual jackpot comparison report;
e) Theoretical hold vs. actual hold comparison with variances;
f) Significant event log for each electronic gaming device;
g) A network topology report;

h) A network status report that indicates, at a minimum, the status of devices interfaced within the communication network globally and locally; and,
i) Security events

10.00 Security Requirements

10.01 Access Control

The entire system shall maintain all accounting information, game data, reporting and other information critical and non-critical in a secure manner. Access shall be designated in a hierarchal manner with the appropriate password, PIN protection and any other safeguards deemed applicable by SLGA.

The central system shall be designed with security and audit ability in mind to enable limited, controlled and monitored use of personnel. Reports and other system output must be available to authorized individuals only.

The central system application and operation software must provide the ability to manage individual user privileges, perform system related functions, and view information. Access rights must be granted specifically and not by default.

The central system must have a method to maintain a system access listing for all authorized users that reflects the access privileges of all authorized users. This listing may be maintained electronically or in printed form (i.e., hard copy). System access must be limited to authorized individuals only, and only at the appropriate level. At a minimum, the system access listing must include the user's name, position, level of authority, authorized functions, and date the authority was granted. All authorized users must be reflected on the system access listing which includes any vendor personnel who have onsite access rights and/or remote access privileges. (All remote access, both during and subsequent to the test period, must be documented on an on-going basis.)

The central system must support either:
a) A hierarchical role structure whereby user and password define program;
b) Individual menu item access; or
c) Logon program/device security based strictly on user and password or PIN.

The central system shall maintain a configurable log of access to alert and trace system activity to specific users which includes:
i) Identification;
ii) Date and time signed in;
iii) Date and time signed out;
iv) What change was made;
v) Which data was affected; and
vi) The original data.

Additionally, there should be a provision for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts. There must be

comprehensive password protection at both the operating system and application level that includes, but isn't limited to:

a) The capability to force a password expiration;
b) Encrypt passwords;
c) No password display;
d) Allow users to change their own passwords; and
e) Force the format of password structure.

10.02 Personal Identification Number (PIN) Management

If PINs are used in any manner within an electronic gaming device and/or the support system, the PIN creation algorithm, its implementation and operational procedures (i.e. PIN changes, database storage, security and distribution) must all be approved. The storage of PINs must be in an encrypted non-reversible form. This means that if a person reads the file that stores the PIN data, he/she must not be able to reconstruct the PINs from that data even if he/she knows the PIN creation algorithm.

10.03 System Upgrades and Modifications

Site operators or designated agents of SLGA are responsible for all system upgrades and system modifications, and for the accuracy and integrity of system data subsequent to the upgrade or modification. Relevant information for these activities must be documented.

10.04 System Application Controls

The central system must have adequate application controls in place to assure the accuracy of data input, integrity of system processing, and validity of system output. Some examples of these types of controls include passwords to restrict data input to authorized users, using parameters or reasonableness checks to verify the integrity of system processing, and using control totals on reports for comparison to input figures.

10.05 Data Alteration

The central system shall not permit the alteration of any accounting or significant event log information that was properly communicated from the electronic gaming device without supervised access controls. In the event financial data is changed, an audit log must be capable of being produced to document:

a) Data element altered;
b) Data element value prior to alteration;
c) Data element value after alteration;
d) Time and date of alteration; and
e) Personnel that performed alteration (user login).

10.06 Database and Validation Component Security

Once the validation information is stored in the database, the data may not be altered in any way. The validation system database must be encrypted or password-protected and should possess a **non-alterable user audit trail** to log database access. Further, the normal operation of any device that holds ticket information shall not have any options or method that may compromise ticket information. Any device that holds ticket information in its memory shall not allow removing of the information unless it has first transferred that

information to the database or other secured component(s) of the validation system. See **Section 5.00 'Database Requirements'** for further information.

10.07 Slot Program Verification Requirements

If central system gaming device verification is supported, a central system shall provide this functionality to check electronic gaming device software. The following information must be reviewed for validity prior to implementation:

a) Software signature algorithm(s); and

b) Data communications error check algorithm(s).

10.08 Verification Algorithm Timing

If central system gaming device verification is supported, verification shall be user initiated or triggered by specific significant event(s) on the electronic gaming device. To ensure complete coverage verification should be performed after each of the following events:

a) Power loss to an electronic gaming device and subsequent power up; and

b) Restoration after communication loss.

The signature checking process must take precedence over any other electronic gaming device operations. This means that the process cannot be interrupted by any other electronic gaming device operations.

10.09 Signature Calculations

If supported, software signatures that are calculated on all electronic gaming devices, are to be validated by central system network.

10.10 Minimum Signature Algorithm Requirements

If central system gaming device verification is supported, a signature algorithm must meet the following requirements:

a) It must combine all of the contents of the software or data being processed (inclusive of any contiguous blank(s) and unused area(s) within the device) (i.e. each and every bit of the contents must influence the signature result);

b) It must combine the bits in a complicated and cross-interactive manner. (An example of such a technique is the cyclic redundancy check (CRC) method);

c) Use of primitive techniques will not be acceptable. Such techniques include (but are not limited to):

i. A parity check (regardless of whether the parity check implements 'exclusive-OR arithmetic' or 'add-arithmetic'); or

ii. A checksum (regardless of whether the checksum produces 8-bit results or 16-bit results).

d) It must produce a result of at minimum16-bits in width. The algorithm must detect at least 99.995% and preferably 99.998% of all possible data errors; and

e) The signature algorithm must be:

i. Fast and efficient, and

ii. Able to process both individual software and fixed data components and entire software suites.

10.11 Signature Seeding

If central system gaming device verification is supported:

a) Signature algorithm "seeds" are to be supplied by the initiator of the signature request at the time of activation.
b) The following principles must apply to signature seeding:
i. The "seed" information is to be at minimum16 bits in length; and
ii. The "seed" information is to influence the behaviour of the algorithm in a non-trivial way.

10.12 Signature Calculation Requirements

If central system gaming device verification is supported
a) If the normal signature check of the entire program exceeds sixty (60) seconds or times out, a strategy of another immediately attempting a second signature check request of the electronic gaming device programming is required. If no check is successful, a failure to verify shall be logged as a priority security event.
a) Signature checks are not required for programming that provides non-critical gaming functions. Examples include: graphics and sound programming.
c) A signature check of the entire range of the program must be performed for an electronic gaming device when any of the following events happen:
ii. The signature seed set is changed at the interface device;
iii. New firmware (programming) is installed in the electronic gaming device;
iv. New software is downloaded to the electronic gaming device;
v. A electronic gaming device power failure. Note that a signature check of only the secure areas of the program may be approved, but a background signature check of the entire program range must be immediately initiated and validated upon completion;
vi. A RAM reset has occurred; or
vii. The logic area cabinet door has been shut (after being opened);
d) Additional to the situations listed above, all electronic gaming device PSD's (i.e. electronic gaming device with storage mediums that support program data downloading) must have central system initiated signature validations scheduled at least once (1) per day.

11.00 Additional System Features

11.01 FLASH Download Requirements

If supported (but not required), a central system may utilize FLASH technology to update interface device software if all of the following requirements are met and are subject to the conditions set for in **Section'10.07 SLOT PROGRAM VERIFICATION REQUIREMENTS'**:
a) FLASH download functionality must be, at a minimum, password protected. The central system can continue to locate and verify versions currently running but it cannot load code that is not currently running on the system without user intervention;
b) A non-alterable audit log must record the time/date of a FLASH download and some provision must be made to associate this log with, which version(s) of code was downloaded, and the user who initiated the download. A separate FLASH audit log report would be ideal; and
c) All modifications to the download executable or flash file(s) must be submitted to an independent testing laboratory for approval. At this time, an independent testing laboratory will perform a FLASH download to the system existing at the testing laboratory and verify

operation. The laboratory will then assign signatures to any relevant executable code and flash file(s) that can be verified by an investigator in the field. Additionally, all flash files must be available to SLGA to verify the signature.

The above refers to loading of new executable code only. Other program parameters may be updated as long as the process is securely controlled and subject to audit.

11.02 Remote Access Requirements

If supported, a central system may utilize password controlled remote access to a central system as long as the following requirements are met:
a) Remote access user activity log is maintained depicting logon name, time/date, duration, activity while logged in;
b) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);
c) No unauthorized access to database other than information retrieval using existing functions;
d) No unauthorized access to operating system;
e) If remote access is to be continuous basis then a network filter (firewall) should be installed to protect access;
f) Physical segregation and methodology of system equipment interfacing will be implemented to prevent unauthorized access into the central system, and
g) Anti-virus protection will be built in where appropriate, and the system shall allow for regular anti-virus updates to be installed.

11.03 System Interfaces

If a weigh scale interface or currency counter interface is utilized, the central system must allow methods for contingency plans that address the manner of reconstructing drop data in the event the interface fails. These methods must include a reconciliation between the weigh scale and/or currency counter and the system-generated reports. These methods must also include contingency plans in the event the weigh scale itself (or currency counter) malfunctions.

11.04 Memory Capacity

SLGA recognizes the fact that it is difficult to determine the memory capacity requirements of the central system. However, the manufacturer shall ensure that every attempt is made to make a reasonable estimation of required capacity such that the Central System shall be equipped with the appropriate amount of memory to adequately handle all database requirements and operational requirements necessary to operate.

11.05 System Scalability

a) **Software and Hardware** - The system must be designed such that it readily accepts software and hardware enhancements.
b) **Modularity** - The central system must be designed to facilitate the ability to add additional gaming products and functions without the risk of affecting the operation of system components.

11.06 Back up and Recovery

a) **Back up** - The central system must operate in a fault tolerant manner where a hardware or software related failure does not impact the continued operation of the central system or the gaming devices associated with it. The central system shall have sufficient redundancy and modularity so that if any single component or part of a component fails, gaming can continue. There shall be redundant copies of each log file or system database or both on the central system with open support for backups and restoration.

b) **Recovery Requirements** - In the event of a catastrophic failure when the central system 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:

i. Priority events;
ii. Accounting information;
iii. Auditing information; and
iv. Specific site information such as slot file, progressive set-up, etc.

If possible, the software will be capable of automatically rebuilding in the event of a hard drive failure.

11.07 Other Hardware

The central system may be designed to permit the use of additional hardware not associated directly with gaming devices. Types of hardware that fit into this category, are, but not limited to: redemption kiosks, automated teller machines (ATM), "quick jacks," etc.

If utilized, these devices must use a communication protocol consistent with the requirements set forth within this document and shall not have the capacity to write information directly to the gaming database.

Additionally, any hardware utilized in this manner must be tested by an approved independent gaming laboratory before being approved for use in Saskatchewan.

12.00 Ticket Validation

12.01 Validation

A ticket validation system may be entirely integrated into a central system or exist as a entirely separate entity. Ticket validation systems are generally classified into two types: bi-directional ticket systems that allow for electronic gaming device ticket insertion and ticket out only systems that do not allow this. This section primarily concerns bi-directional ticket systems. Where ticket out only systems are utilized, some of the following in this section may not apply.

12.02 Payment by Ticket Printer

Payment by ticket printer as a method of credit redemption on an electronic gaming device is only permissible when the electronic gaming device is linked to an approved validation system or central system that allows validation of the printed ticket. Validation information shall come from the validation system or central system using a secure communication

protocol based on the criteria set forth in this document. See Section 12.14 'Offline Ticket Redemption.

12.03 Ticket Information

A ticket shall contain the following printed information at a minimum:
a) Casino name;
b) Machine number;
c) Date and time (24hr format);
d) Alpha and numeric dollar amount of the ticket;
e) Ticket sequence number;
f) Validation number;
g) Bar code or any machine readable code representing the validation number;
h) Type of transaction or other method or differentiating ticket types; and
i) Indication of an expiration period from date of issue, or date and time the ticket will expire (24hr format).

12.04 Ticket Types

If electronic gaming device ticket generation is supported while not connected to the validation system, a ticket system must generate two different types of tickets at minimum. On-line and off-line types are denoted respectively by ticket generation either when the validation system and electronic gaming device are properly communicating or the validation system and electronic gaming device is not communicating properly. When a patron cashes out of an electronic gaming device that has lost communication with the validation system, the electronic gaming device must lockup and, print an offline ticket. The offline ticket must be visually distinct from an on-line ticket either in format or content while still maintaining all information requirements.

12.05 Ticket Issuance

A ticket can be generated at an electronic gaming device through an internal document printer, at a player's request, by redeeming all credits. Tickets that reflect partial credits may be issued automatically from an electronic gaming device. Additionally, cashier/change booth issuance is allowed if supported by the validation system.

12.06 Online Ticket Redemption

Tickets may be inserted in any electronic gaming device participating in the validation system providing that no credits are issued to the electronic gaming device prior to confirmation of ticket validity. The customer may also redeem a ticket at a cashier/change booth or other approved validation terminal.

The central system shall be capable of allowing "cross validation," or ticket redemption at multiple casino sites should an operator choose to activate this feature.

12.07-12.10 Reserved for amendments

12.11 Cashier/Change Booth Operation

All validation terminals shall be user and password controlled. Once presented for redemption, the cashier shall:
a) Scan the bar code via an optical reader or equivalent;

b) Input the ticket validation number manually; and
c) Print a validation receipt after the ticket is electronically validated.

12.12 Validation Receipt Information

The validation receipt at a minimum shall contain the following printed information:
a) Machine number;
b) Validation number;
c) Date and time paid;
d) Amount;
e) Cashier identifier; and
f) Casino name.

12.13 Invalid Ticket Notification

The validation system or central system must have the ability to identify these occurrences and notify the cashier that one of the following conditions exists:
a) Serial number cannot be found on file (stale date, forgery, etc.);
b) Ticket has already been paid; or
c) Amount of ticket differs from amount on file (requirement can be met by display of ticket amount for confirmation by cashier during the redemption process).

12.14 Offline Ticket Redemption

If the on-line data system temporarily goes down and validation information cannot be sent to the validation system or central system, an alternate method of payment must be provided either by the validation system possessing unique features (validity checking of ticket information in conjunction with a local database storage) to identify duplicate tickets and prevent fraud by reprinting and redeeming a ticket that was previously issued by the electronic gaming device or use of an approved internal controls and procedures established by the operator. See Section 12.02 'Payment by Ticket Printer.'

12.15 Reporting Requirements

The following reports shall be generated at a minimum and reconciled with all validated/redeemed tickets:
a) Ticket issuance report;
b) Ticket redemption report;
c) Ticket liability report;
d) Ticket drop report;
e) Jackpot ticket report;
f) Transaction detail report must be available from the validation system that shows all tickets generated by an electronic gaming device and all tickets redeemed by the validation terminal or other electronic gaming device; and
g) Cashier report to detail sum of tickets paid by cashier or validation unit.

13.00 Progressive Jackpot Systems

13.01 Progressive Jackpot Systems Defined.

A progressive jackpot is an award for a winning or non-winning (e.g. mystery jackpot) play of the game. A bonus game where certain circumstances are required to be satisfied, prior to

awarding a fixed bonus prize, is not a progressive gaming device and is not subject to these procedures.

13.02 General

The rules within this section shall allow for securely changing of any of the associated parameters. **All topics covered in this section are subject to all of the standards outlined within this document**. Additionally, the communication process must be robust and stable enough to secure each progressive transaction such that a failure event(s) can be identified and logged for subsequent audit and reconciliation.

13.03 Progressive Meter/Display Requirements

One or more progressive gaming device(s) shall be linked, directly or indirectly, to a mechanical, electrical, or electronic device, including a video display, if applicable, that shows the payoff which increments at a set rate of progression as credits are wagered. This device is the progressive meter. For games that have progressives such as 'mystery jackpot', the payoff does not have to be displayed to the player although, there should be an indication as to this type of feature on the game.

13.04 Progressive Displays

A progressive meter shall be visible to all players who are playing a device, which may potentially win the progressive amount if the progressive jackpot combination appears, except for 'mystery jackpots.' A player shall know that he is playing a progressive game and not have to play the max bet amount to find out. The above are parameters that are verified on-site. The following rule shall apply to all progressive meter displays:
The progressive meter shall display the current total of the progressive jackpot in the monetary value or credits (the monetary value may vary for multi-site progressive displays due to lag-time in communication). Because the polling cycle does cause a delay, the jackpot meter does not need to precisely show the actual monies in the progressive pool at each instance.

13.05 Types of Updating Displays

The use of odometer and other "paced" updating displays are allowed. The progressive meter shall display the winning value within 30 seconds of the jackpot being recognized by the central system. In the case of the use of paced updating displays, the system jackpot meter shall display the winning value after the jackpot broadcast is received from the central system.

13.06 Progressive Display Digital Limitations

If the progressive meter(s) progresses to its maximum display amount, the meter shall freeze and remain at the maximum value until awarded to a player. This can be avoided by setting the jackpot limit in accordance with the digital limitations of the sign.

13.07-13.10 Reserved for amendments

13.11 Progressive Controller Requirements

If specific 'progressive controllers are utilized, any progressive system shall meet the game standards set forth in this document and **SLOT MACHINE INTEGRITY STANDARDS.** The requirements are intended to apply equally to one progressive gaming device linked to a

progressive controller or is internally controlled, as well as several progressive gaming devices linked (master/slave configuration) to one progressive controller within one casino or multiple casinos.

13.12 Progressive Controller Description

If 'progressive controllers are utilized: A progressive controller is all of the hardware and software that controls all communications among the devices that calculates the values of the progressives and displays the information within a progressive gaming device link (if applicable – progressive gaming device(s) may be internally controlled) and the associated progressive meter. This equipment includes but is not limited to PC-based computers, wiring, collection nodes, etc.

13.13 Random Number Generator/RNG Seeding.

If the progressive system utilizes a random number generator for a "mystery" progressive or other progressive "random" prizes, then the first seed shall be randomly determined by an uncontrolled event. This event shall be transparent to the user and shall not be known. The value will conform to the specified operating guidelines of the progressive system. After every user access to the parameter menu within the progressive system, there shall be a random change in the RNG process (new seed). This will verify the RNG doesn't start at the same value, every time. It is permissible not to use a random seed, however, the manufacturer must ensure that previous values will not synchronize with current or future values.

Recognized tests shall be used to determine whether or not the random values produced by the random number generator pass the desired confidence level of 99%. These tests may include, but are not limited to:

a) Chi-square test;
b) Equi-distribution (frequency) test;
c) Gap test;
d) Overlaps test;
e) Poker test;
f) Coupon collector's test;
g) Permutation test;
h) Kolmogorov-Smirnov test;
i) Adjacency criterion tests;
j) Order statistic test;
k) Runs tests (patterns of occurrences should not be recurrent);
l) Interplay correlation test;
m) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game);
n) Tests on subsequences; and
o) Any other tests deemed a requirement by SLGA.

Progressive systems shall not utilize an electro-mechanical system based random number generator (RNG) 'mystery' awards or any other application of a random number generator.

13.14-13.20 Reserved for amendments

13.21 Progressive Communication Requirements

All topics covered in this section are also subject to the standards set forth in Section 6.00 of this document to ensure the highest level of integrity possible.

13.22 Synchronization Feature

If multiple clocks are supported, the central system shall have a facility whereby it is able to update all clocks in central system components. This includes: clocking in, cashless, bonus, progressive and promotional systems. All internal clocks shall be synchronized by the central system.

13.23 Setting the Value Amounts

The method by which system jackpot parameter values are modified or entered is to be secure. All progressive gaming devices or any approved progressive system component shall capture, the following information for each progressive prize offered (if applicable):

a) Current Value: current prize amount;
b) Overflow: amount exceeding limit;
c) Hits: number of times this progressive was won;
d) Wins: total value of wins for this progressive or a history of the last 25 progressive hits;
e) Base: starting value;
f) Limit: jackpot limit value (if the Jackpot is capped at a maximum limit, this standard does not require to add the overflow amounts to the next starting value and will be determined on a casino-by-casino basis);
g) Increment: percentage increment rate;
h) Secondary Increment: percentage increment rate after limit is reached;
i) Hidden Increment: percentage increment rate for the reserve pool (the next base amount shall be computed or posted to advise the player of this contribution);
j) Reset Value: the amount the progressive resets to after the progressive is won;
k) The participating gaming devices;
l) Reference numbers; and
m) Denomination multipliers (if applicable).

NOTE: Any change to the jackpot amount must conform to casino internal control procedures.

13.24 Progressive Controller Program Interruption

After a program interruption (e.g. power down), the software shall be able to recover to the state it was in immediately prior to the interruption occurring.

13.25 Progressive Resumption

On program resumption, the following procedures shall be performed as a minimum requirement:

a) Any communications to an external device shall not begin until the program resumption routine, including self-tests, is completed successfully; and
b) Progressive system control programs shall test themselves for possible corruption due to failure of the program storage media. The authentication may use the checksum, however, it is preferred that the cyclic redundancy check (CRC) calculations are used as a minimum (at

least 16 bit). Other test methodologies shall be acceptable if at a comparable level of integrity.

13.26 Communications for Signaling of a Jackpot

There shall be a secure, two-way communication protocol between the main game processor board and progressive. In addition, the progressive system shall be able to:
a) Send to the electronic gaming device the amount that was won for metering purposes; and
b) Constantly update the progressive display as play on the link continues.

13.27 Monitoring of Credits Bet

During the 'normal operating mode' of progressive gaming devices, the progressive controller shall continuously monitor each device on the link for credits bet and shall multiply the same by the rate of progression and denomination in order to determine the correct amounts to apply to the progressive jackpot. This shall be 99.99% accurate.

13.28 Progressive Controller Required Meters

The progressive controller or other approved progressive system component shall keep the following information in non-volatile memory, which shall be displayed on demand. Additionally, meters shall be 99.99% accurate including:
a) The number of progressive jackpots won on each progressive level if the progressive display has more than one (1) winning amount;
b) The cumulative amounts paid on each progressive level if the progressive display has more than one (1) winning amount;
c) The maximum amount of the progressive payout for each level displayed;
d) The minimum amount of the progressive payout for each level displayed; and
e) The rate of progression for each level displayed.

13.29 Controller and Display Functions During Progressive Jackpot Win

When a progressive jackpot is recorded on an electronic gaming device, which is attached to the progressive controller, the progressive controller shall allow for the following to occur on the device and/or progressive display:
a) Display of the winning amount;
b) Display of the electronic gaming device identification that caused the progressive meter to activate if more than one (1) electronic gaming device is attached to the controller; and
c) The progressive controller shall automatically reset to the reset amount and continue normal play.

13.30 Progressive Jackpot Amount

The initial amount of a progressive jackpot shall begin at or above an award for that particular gaming device that makes the entire meter payout greater than the minimum percentage requirement of the individual gaming device. See also **Section 4.30 Software Requirements for Percentage Payout in ‘‘SLOT MACHINE INTEGRITY STANDARDS.**

13.31-13.37 Reserved for amendments

13.38 Progressive Controller Error Conditions

When a controller error occurs, it is preferred that it alternates the displays, or equivalent, between the current amount and an appropriate error message that is visible to all players, or

can alert the casino to the error condition. If the following events occur, the game that is using the progressive is to be disabled, and an error shall be displayed on the progressive meter, other approved progressive system component or gaming device:
a) During a 'communication failure(s)', see also "communication failure" section;
b) When a controller checksum or signature has failure;
c) When a controller's RAM or PSD (program storage device) mismatch or failure occurs;
d) When the current amount is larger than the limit, see also "jackpot limits" section;
e) When the jackpot configuration is lost or is not set;
f) If there has been an unreasonable amount of credits bet (an unreasonable amount of credits bet is defined by the progressive set up which is based on the number of bets and number of machine(s)); or
g) If the game meters are validated against the controller's meters (via communications between the game board and controller) and they do not reconcile.

13.39 Transferring of Progressive Jackpot

The progressive controller shall have a secure means of transferring a progressive jackpot and/or prizes to another progressive controller or other approved progressive system component. Transferring of progressive jackpots must meet the internal control procedures approved by SLGA.

13.40 Time Limits

Progressive controller may have the ability to set time limits that limit the time the progressive is available.

13.41 Gaming Device Requirements when any Progressive is Awarded

When a progressive prize has been awarded, the gaming device or other approved progressive component shall perform the following:
a) An appropriate message shall be displayed;
b) Unless the prize is transferred to the player's credit meter the software and game shall lockup until the award has been paid by the attendant;
c) All progressive related meters must be updated, see also 'slot standards'; and
d) In the case of a player winning a 'mystery jackpot', there must be a light or an alarm so the player doesn't abandon the machine, not knowing they've won an award.

13.42 Progressive Gaming Device Metering Requirements

The electronic gaming device is required to update its electronic meters to reflect the winning progressive jackpot amount consistent with these procedures and **Section 4.56 Electronic Accounting and Occurrence Meters in "SLOT MACHINE INTEGRITY STANDARDS."** Progressive wins may be added to the credit meter if either:
a) The credit meter is maintained in monetary value or credits;
b) The progressive meter is incremented to whole credit amounts; or
c) The prize, in monetary value, is converted to credits on transfer to the player's credit meter in a manner that does not mislead the player. The conversion from monetary value to credits must always round up.

13.43 Progressive Percentage Requirements and Odds

The rules within this section shall not supersede **Section 4.31 'Progressive Game Calculations' in "SLOT MACHINE INTEGRITY STANDARDS."**

13.44 Multiple Site Progressive Requirements

This section shall set forth the technical requirements for "multi-site progressive gaming devices." Multi-site progressive gaming devices are interconnected in more than one casino. The purpose of a Multi-site progressive system is to offer a common progressive jackpot (system jackpot) at all participating locations.

13.45 Location of Central Monitoring System

It is recommended that site operators/agents take the necessary steps to enact "due diligence" by ensuring that the area containing the central computer shall be equipped with a surveillance system that must meet internal control procedures.

13.46 Method of Communication for Multi-Site Gaming Devices

The method of communication shall be a non-shared, dedicated line or equivalent. Dial-tone systems may be used as long as devices at the local site would not be able to be disabled from another outside line or manipulated by any other means. When the method of communication is a shared line, appropriate encryption and security must be in place to avoid corruption or compromise of data.

13.47 Data Collection Requirement

Multi-site systems shall ensure that security information and the amounts wagered information is communicated, at least once every 15 seconds for terrestrial lines (dedicated phone lines).

13.48-13.51 Reserved for amendments

13.52 Multi-Site Encryption/Security Method

All multi-site property systems shall utilize an encryption or security method that has been approved by SLGA, or by an approved laboratory. Such methods shall include the use of different encryption "keys" or "seeds" so that encryption can be changed in a real-time fashion. Refer to Section 6.00 Communication for further information.

13.53 Multi-Site Monitoring

The central system must be able to monitor the meter readings and error events of each device such that the on-line security system requirement for active gaming devices is not altered in any way.

13.54 Central Monitoring System Power Supply

The central computer site shall be equipped with non-interruptible power supply that will allow the central computer to conduct an orderly shut down if the power is lost.

13.55 Communication Failure

A gaming device shall disable itself and suspend play if communication is lost to the local collection unit and security hub. The gaming device may resume play only when communication to the local hub is restored. If the communication is lost between the local hub and the central computer, the gaming device may continue to play. However, once communications are re-established, the system wide totals are to be updated; not

withstanding this rule if the communication is lost for more than 24 hours and the site must be shut down.

13.56 Central Monitoring System Required Reports

Any "multi-site" system shall supply, as requested, the following reports:
a) Progressive Summary: A report indicating the amount of, and basis for, the current jackpot amount (the amount currently in play);
b) Aggregate Report: A report indicating the balancing of the system with regard to system wide totals; and
c) Payoff Report: A report that will clearly demonstrate the method of arriving at the payoff amount. This will include the credits contributed beginning at the polling cycle, immediately following the previous jackpot and will include all credits contributed up to and including the polling cycle which includes the jackpot signal.
NOTE: Credits contributed to the system after the jackpot occurs in real-time, but during the same polling cycle, shall be deemed to have been contributed to the progressive amount prior to the jackpot. Credits contributed to the system subsequent to the jackpot message being received, as well as credits contributed to the system before the jackpot message is received by the system, but registered after the jackpot message is received at the system, will be deemed to have been contributed to the progressive amount of the next jackpot, if applicable.

13.57 Multi-Site System Meter Readings

All meter reading data shall be obtained in real time in an on-line automated fashion. When requested to do so, the system shall return meter readings on all gaming devices attached to the system. The meter readings shall be identical to the meter information retained in the gaming device(s) accounting meters. Manual reading of meter values may not be substituted for these requirements.

13.58 Multi-Site System Door Monitoring

The Multi-Site Progressive system shall have the ability to monitor entry into the front door of the gaming device and report it to the central system IMMEDIATELY.

13.59 Jackpot Win During Poll Cycle

If a jackpot is recognized in the middle of a system-wide poll cycle, the overhead display may contain a value less than the aggregated jackpot amount calculated by the central system. The credit values from the remaining portion of the poll cycle will be received by the central system but not the local site, in which case the jackpot amount paid will always be the higher of the two reporting amounts.

13.60 Multiple Jackpots During the Same Polling Cycle

When multiple jackpots occur, where there is no definitive way of knowing which jackpot occurred first, they will be deemed to have occurred simultaneously; and therefore, SLGA shall adopt procedures for payment of such jackpot occurrences. In addition, if there is a communication failure as described in **Section 6.00 "Communication,"** a winning player wagering at a non updated site may also be eligible to a jackpot amount.

13.61 Diagnostic Tests on a Progressive Gaming Device

The progressive system will have built in features permitting diagnostic testing of the said system and a specific gaming device progressive interface (if applicable). While in diagnostics mode, the progressive system shall clearly indicate on applicable signage that it is “test” mode, and shall send an event signal to the central system indicating its status. No progressive prizes or progressive awards shall be available while the progressive system is in diagnostics mode.

14.00 Bonusing Systems

14.01 Bonus System Defined

Bonusing systems are comprised of gaming devices that are configured to participate in electronically communicated bonus award payments from a central system, and the central System that controls the bonus award issuance parameters. The bonus central system provides designated gaming devices with additional features that entitle players to special bonus awards based on events triggered by the gaming device. In other words, bonus awards are a derivative of an existing casino feature whereby game events may result in additional pays to those described on the paytable (artwork or help screens). Facilities now exist to support these awards at a gaming machine utilizing protocol commands for direct credit transfers to the gaming machine as the patron is playing the device. Bonus awards are those based on a gaming machine event or some external trigger which do not include triggers based upon specific patron activity. A bonus award is typically won based on several criteria: a variable amount of play occurring on a group of participating gaming machines or achieving a winning combination during a specific time frame. Examples include: multiplied jackpots, whereby the central system is able to instruct the gaming machine to multiply all wins within a specified range by a specified value or an n^{th} coin award is won when a percentage of play on participating gaming machines reaches a randomly selected value.

14.02 General

The rules within this section shall be implemented by the central system to allow for securely changing of any of the associated parameters. **All topics covered in this section are subject to all of the standards outlined within this document**. Additionally, the communication process must be robust and stable enough to secure each transaction such that failure event(s) can be identified and logged for subsequent audit and reconciliation.

14.03 Configuring Bonus Transactions on a Gaming Device

Since a bonusing feature would impact the electronic accounting meters, any gaming device that allows bonusing gaming as a selectable feature must conform to the configuration setting requirements outlined within ‘slot standards’.

14.04 Audit Trails for Bonusing Transactions

Bonus gaming devices must have the ability to recall the last twenty-five (25) monetary transactions received from the host system. However, if a gaming device has cashless or host-promotional features, or both, enabled simultaneously with bonus features, a single 100-event log would suffice. The following information must be displayed:

a) The transaction value;
b) The time and date; and
c) Unique transaction identification or number.

14.05 Meter Requirements for Bonusing Gaming Devices

Bonus gaming devices must incorporate electronic accounting meters that conform to the following electronic metering requirements:

a) The operation of the mandatory electronic accounting meter, "coins-out" as described in ‘Slot Machine Integrity Standards’, shall reflect bonus wins, if the host pays those bonus wins to the game (i.e. not handpaid);

b) The operation of the mandatory electronic accounting meter, "handpays" as described in slot standards, shall reflect bonus wins that are handpaid by the gaming device; and
c) In addition to the "coins-out" meter being incremented, the following additional specific bonus meters will be added:

i. Total bonus in (received by game) meter; and
ii. Total bonus handpaid meter (bonus award received by game that forced handpay condition.

NOTE: If conditions exist wherein a bonus award is transferred to a gaming device, and results in a handpay, then this meter must increment for the value of the bonus award. Further, where this meter is not supported in the protocol, this requirement may be waived as long as there is a method to audit the bonus awards that are handpaid.

14.06 Central System Audit Trails

The central system shall have the ability to produce logs for all complete bonus transactions to include the same information required on gaming machine audit logs. In addition, these logs shall be capable of being filtered by:
a) Machine number;
b) Time/date; and
c) Type.

14.07 Reports

The system shall have the ability to produce the following reports:
a) Bonus Summary and Detail Reports. These reports shall include transaction information indicating the gaming machine number, amount, date/time and type of bonus;
b) Bonus Meter Reconciliation Summary and Detail Reports. These reports shall provide reconciliation of each participating gaming machine bonus meter(s) against central system's bonus activity; and
c) Auditing Report. This report shall provide modification details whenever critical parameters are modified.
NOTE: There must be a report or method that would allow the comparison of the theoretical hold percentage of the bonusing gaming device to the actual hold of the device.

14.08 – 14.11 Reserved for amendments

14.12 Notification of a Bonus Award

The method of bonus win notification, at or near the gaming device, can include any combination of host messaging, sounds, or visual indicators as long as deemed acceptable. Since bonuses are awarded directly to the gaming device, the gaming device itself shall reflect the amount of the bonus win. Additionally, electronic accounting meters, and logs will reflect all bonus transactions accordingly.

14.13 Communication Requirements.

All topics covered in this section are also subject to the standards set forth in **Section 6.00 'Communication'** to ensure the highest level of integrity possible.

14.14 Communication Failure

Messages must be either displayed to the patron or be available under a diagnostic function, either at the game or system level, which would indicate the reason for any bonus transaction failure due to a communication failure.

NOTE: In this circumstance, the bonusing system must recognize failure of bonus win payment to be paid to the gaming device, and notify appropriate casino personnel so manual procedures can be implemented to ensure proper payment.

14.15-14.20 Reserved for amendments

14.21 Modification of Critical Parameters

All changes to factors that may impact bonus redemption frequency or amount must be logged indicating:

a) Who made the change;
b) The altered parameter;
c) The time and date of change;
d) The parameter value before and after the change; and
e)The reason for the parameter adjustment.

The Bonusing system shall be subject to the requirements set forth in the section 'Access Control' outlined in slot systems.

14.22 Prevention of Unauthorized Transactions

The following minimal controls shall be implemented by the central system to ensure that games are prevented from responding to commands for crediting outside of properly authorized bonus transactions (hacking):

a) The network hubs are secured (either in a locked/monitored room or area) and no access is allowed on any node without valid login and password;
b) The number of stations where critical bonusing applications or associated databases could be accessed is limited; and
c) The users who have the requisite permission levels/login to adjust critical parameters are limited.

See section 'Access Control' outlined in slot systems for further information.

14.23 Synchronization Feature

If multiple clocks are supported, the central system shall have a facility whereby it is able to update all clocks in central system components. This includes clocking in: cashless, bonus, progressive and promotional systems. All internal clocks shall be synchronized by the central system.

14.24 Diagnostic Tests on a Bonusing Gaming Device

The bonusing system will have built in features permitting diagnostic testing of the said system and a specific gaming device bonus interface (if applicable). While in diagnostics mode, the bonusing system shall clearly indicate on applicable signage that it is "test" mode, and shall send an event signal to the central system indicating its status. No bonus prizes or bonus awards shall be available while the bonusing system is in diagnostics mode.

14.25 Random Number Generator

RNG Seeding. If the bonus system makes use of a random number generator, the first seed shall be randomly determined by an uncontrolled event. This event shall be transparent to the user and shall not be known. The value will conform to the specified operating guidelines of the bonus system. After every user access to the parameter menu within the bonus system, there shall be a random change in the RNG process (new seed). This will verify the RNG doesn't start at the same value, every time. It is permissible not to use a random seed; however, the manufacturer must ensure that previous values will not synchronize with current or future values. Recognized tests may be used to determine whether or not the random values produced by the random number generator pass the desired confidence level of 99%.

Bonus systems shall not utilize an electro-mechanical system based random number generator (RNG).

15.00 Cashless Systems

15.01 Cashless Systems Defined

A cashless system is a central system that utilizes technology to allow players the ability to upload, download, transfer and redeem credits or cash independently on the gaming floor via other gaming devices and kiosks.

15.02 General

The rules within this section shall be implemented by the central system to allow for securely changing of any of the associated parameters. **All topics covered in this section are subject to all of the standards outlined within this document**. Additionally, the communication process must be robust and stable enough to secure each cashless transaction such that failure event(s) can be identified and logged for subsequent audit and reconciliation.

15.03 Configuring Cashless Transactions on a Gaming Device

Since a cashless feature would impact the electronic accounting meters, any gaming device that allows Cashless gaming as a selectable feature must conform to **"SLOT MACHINE INTEGRITY STANDARDS."**

15.04 Audit Trails for Cashless Transactions

Cashless gaming devices must have the ability to recall the last twenty-five (25) monetary transactions received from the host system and the last twenty-five (25) monetary transactions transmitted to the central system. However, if a gaming device has promotional or host-bonusing features, or both, enabled simultaneously with cashless features, a single 100-event log would suffice. The following information must be displayed:

a) The type of transaction (upload/download);
b) The transaction value;
c) The time and date; and
d) The player's account number or a unique transaction number, either of which can be used to authenticate the source of the funds (i.e. source of where funds came from/went to).

15.05 Meter Requirements for Cashless Gaming Devices

Cashless gaming devices must incorporate electronic accounting meters that conform to the following electronic metering requirements:

a) The operation of the mandatory electronic accounting meters, as mandated in **Section 4.56 'Electronic Accounting and Occurrence Meters' in ''SLOT MACHINE INTEGRITY STANDARDS."** must not be impacted directly for cashless transactions; and

b) Specific cashless electronic accounting meters exist which should increment to indicate:

i. Electronic credits received from the central system---downloaded to game from host.

ii. Electronic credits transmitted to the central system---uploaded from game to host.

15.06 Financial and Player Reports

The system shall have the ability to produce the following financial and player reports:

a) Patron Account Summary and Detail Reports. These reports shall be immediately available to a patron upon request. These reports shall include beginning and ending account balance, transaction information depicting gaming machine number, amount, and date/time;

c) Liability Report. This report is to include previous days starting value of outstanding cashless liability, aggregate cashless-in and out totals, and ending cashless liability;

d) Cashless Meter Reconciliation Summary and Detail Reports. These reports will reconcile each participating gaming device's Cashless meter(s) against the Central System's Cashless activity; and

e) Cashier Summary and Detail Reports. To include patron account, buy-ins and cash-out, amount of transaction, date and time of transaction.

15.07 Central System Security Requirements

The rules within this section shall be implemented by the central system to allow for changing of any of the associated parameters or accessing any patron account. Additionally, the communication process used by the gaming device and the central system must be robust and stable enough to secure each cashless transaction such that failure event(s) can be identified and logged for subsequent audit and reconciliation.

15.08-15.11 Reserved for amendments

15.12 Encryption

Security messages that traverse data communications lines must be encrypted (optional) using the best known form of encryption available at the time. The intent is that communications be demonstrably secure against crypto-analytic attacks. Refer to **Section 6.06 'Encryption'** for further details.

15.13 and 15.14 Reserved for amendments

15.15 Security Levels

The number of users that have the requisite permission levels/login to adjust critical parameters are limited and are subject to the security guidelines outlined in 'Security Requirements' of Central Systems.

15.16 Prevention of Unauthorized Transactions

The following minimal controls shall be implemented by the central system to ensure that games are prevented from responding to commands for crediting outside of properly authorized cashless transactions (hacking):

a) The network hubs are secured (either in a locked/monitored room or area) and no access is allowed on any node without valid login and password;

b) The number of stations where critical cashless applications or associated databases could be accessed is limited; and

c) Procedures shall be in place on the system to identify and flag suspect player and employee accounts to prevent their unauthorized use to include:

i. Having a maximum number of incorrect PIN entries before account lockout;

ii. Flagging and suspension of activity of "hot" accounts where cards have been stolen;

iii. Invalidating accounts and transferring balances into a new account; and

iv. establishing limits for maximum Cashless activity in and out as a global or

v. Individual variable to preclude money laundering.

15.17 Error Conditions

The following sections outline the error conditions that apply to the:

a) Central system. The following conditions must be monitored, and a message must be displayed to the patron at the host card reader for the following:

i. invalid PIN or Player ID (can prompt for re-entry up to maximum allowed); and

ii. account unknown.

b) Gaming device. Any credits on the gaming device that are attempted to be transferred to the central system that result in a communication failure for which this is the only available payout medium (the patron cannot cash out via hopper or ticket printer), must result in a hand-pay lockup or tilt on the gaming device.

15.18 Central System Audit Trails

The central system shall have the ability to produce logs for all pending and completed cashless transactions. These logs shall be capable of being filtered by:

i. Machine number

ii. Patron account; and

iii. Time/date.

15.19 Communication Requirements

All topics covered in this section are also subject to the standards set forth in Section 6.00 Communication of this document to ensure the highest level of integrity possible.

15.20 Transaction Confirmation

The gaming device or host card reader display must be capable of providing confirmation/denial of every cashless transaction initiated. This confirmation/denial must include:

a) The type of transaction (upload/download);

b) The transaction value;

c) The time and date (if printed confirmation);

d) The player's account number or a unique transaction number, either of which can be used to authenticate the source of the funds (i.e. source of where funds came from/went to) [if printed confirmation]; and
e) A descriptive message as to why the transaction did not complete as initiated.
This applies only to denied transactions.

15.21 Full Transfer of all Transactions

If a player initiates a cashless transaction and that transaction would exceed game configured limits (i.e. the credit limit, etc.) then this transaction must be rejected. A partial transaction may never occur.

15.22 – 15.27 Reserved for amendments

15.28 Gaming Device/Card Reader Requirements

The requirements throughout this section apply to gaming devices of the cashless environment. These requirements are in addition to the requirements set forth in **Section 3.96 Card Readers in "SLOT MACHINE INTEGRITY STANDARDS."**

Card Readers

A card input system shall be constructed in such a manner to that protects against vandalism, abuse and fraudulent activity. A card input system must:

a) Not allow card travel paths to be easily altered without leaving evidence of tampering;
b) Have the ability to resist liquid spills;
c) Be designed to resist jams and impaired use that would otherwise render the card useless;
d) Be constructed to detect card insertion and enable software to identify valid or invalid acceptance; and
e) Have mechanisms to allow software to identify and act on significant event such as:
    i. Card acceptor/reader disconnected;
    ii. Card acceptor/reader jammed; and
    iii. Card acceptor/reader malfunctioning.

15.29 Synchronization Feature

If multiple clocks are supported the central system shall have a facility whereby it is able to update all clocks in central system components. This includes clocking in: cashless, bonus, progressive and promotional systems. All internal clocks shall be synchronized by the central system.

15.30 Diagnostic Tests on a Cashless Gaming Device

Controls must be in place for any diagnostic functionality available at the device such that all activity must be reported to the system that would reflect the specific account(s) and the individual(s) tasked to perform these diagnostics. This would allow all cashless diagnostic activity that affect the gaming device's associated electronic meters to be audited by SLGA.

15.31 Player Accounts

All monetary transactions between a supporting gaming machine and the host **must be secured** either by card insertion into a magnetic card reader attached to the host and PIN entry or by other approved protected means (e.g. finger-print recognition). After the player's

identity is confirmed, the device may present transfer options to the patron on the LCD/VFD display of the card reader, which requires selection using a keypad/touchscreen before occurring. Such options would include how many credits the player wishes to "withdraw" and be placed on the machine. Some systems may move the entire player's balance to the machine for play. Once play is complete the player may have the option to move some of the credits back to the account or cash out. Other systems may require that the entire currency value of the credit balance be transferred back to the system.

15.32 Adding Money to a Players Account

Money may be added to this account via a cashier station. Money may also be added by any approved supporting gaming device (through credits won, the insertion of coins, tickets, bills, coupons, etc.)

15.33 Removing Money from a Players Account

Money may be removed from this account either through downloading of credits (currency based) to the gaming device or by cashing out at a cashier's cage.

15.34 Movement of Money

Players may also be afforded the option of moving some of their system credit to the gaming device they are playing through "withdrawal" from the player's account, which is maintained by the system. When they are finished playing, they can "deposit" their balance from the machine onto their player account. Cashless gaming transactions are entirely electronic.

15.35 Personal Identification Number

Usually a casino issues a patron a unique magnetic card and personal identification number (PIN) in conjunction with an account on the system's database, although any method of uniquely identifying patrons could be implemented.

15.36 Account Balance

Current account balance information should be available on demand from any participating gaming device via the associated card reader (or equivalent) after confirmation of patron identity and be presented, in terms of currency, to the patron.

16.00 Promotional Systems

16.01 General Statement

The rules within this section shall be implemented by the central system to allow for securely changing of any of the associated parameters. All topics covered in this section are subject to all of the standards outlined within this document. Additionally, the communication process must be robust and stable enough to secure each promotional transaction such that failure event(s) can be identified and logged for subsequent audit and reconciliation.

16.02 Configuring Promotion Transactions on a Gaming Device

Since a promotional feature would impact the electronic accounting meters, any gaming device that allows promotional gaming as a selectable feature must conform to **"SLOT MACHINE INTEGRITY STANDARDS."**

16.03 Meter Requirements for Promotional Gaming Devices

Promotional gaming devices must incorporate electronic accounting meters that conform to the following electronic metering requirements:

a) The operation of the mandatory electronic accounting meters, as mandated in **Section 4.56 'Electronic Accounting and Occurrence Meters' in "SLOT MACHINE INTEGRITY STANDARDS."** must not be impacted directly for promotion transactions; and

b) The following specific promotional meters will be added:

i. Total promotional awards in (received by game) meter, which includes:

A. Total non-restricted (cashable), promotional in if applicable; and

B. Total restricted (non-cashable), promotional in if applicable.

ii. Total promotional awards out (removed from game and transferred back to player account) meter, if applicable, which includes:

A. Total non-restricted (cashable) promotional out; and

B. Total restricted (non-cashable) Promotional out.

NOTE: If restricted promotional credits and non-restricted credits are co-mingled on one credit meter at a gaming device: when restricted promotional credits are transferred to a game, and that game also has existing cashable credits available, the game MUST pull from the restricted credit balance first during player wagering. All restricted credits must be wagered first before any non-restricted credits are committed. When the non-restricted and aggregate credit balance are paid out; the restricted credit balance remains on the gaming device and must be played off. As well, there shall be a message to the patron either through the gaming device or associated player tracking hardware advising the patron that the remaining balance cannot be cashed out since it was associated with a promotion.

16.04 Identifying a Promotional Device

A patron should be able to identify each machine that supports the promotion by a means left to the discretion of the individual operator (e.g. remove display menu items that pertain to promotional operation for gaming machines not participating; provide a host message indicating promotional capability; or a specific sticker on gaming machines to indicate participation).

16.05 Notification of a Promotional Award

The method of promotional award notification can include any combination of host messaging, sounds, or visual indicators. Since promotional awards are paid directly to the gaming device (if applicable, after player intervention), the gaming device itself shall reflect the amount of promotional awards. Additionally, electronic accounting meters, and logs will reflect all promotional transactions accordingly.

16.06 Disclaimers and Feature Expiration

Any disclaimers such as promotion expiration and their display to the public are also left to the discretion of the individual operator/organization, as they will likely be non-uniform across specific manufacturer implementations.

16.07 – 16.10 Reserved for amendments

16.11 Audit Trails for Promotional Transactions

Promotional gaming devices must have the ability to recall the last twenty-five (25) promotional transactions received from the system and the last twenty-five (25) promotional transactions transmitted to the host system. However, if a gaming device has bonusing or host-cashless features, or both, enabled simultaneously with promotional features, a single 100-event log would suffice. The following information must be displayed:

a) The type of transaction (upload/download) including restrictions (cashable or non-cashable, etc), if utilizing a single 100-event log;

b) The transaction value;

c) The time and date; and

d) The player's account number or a unique identifier, either of which can be used to authenticate the source of the funds (i.e. source of where funds came from/went to).

16.12 Financial Reports

The system shall have the ability to produce the following reports:

a) Patron Promotional Account Summary and Detail Reports. These reports shall include beginning and ending balance(s), transaction information including gaming machine number, amount, date/time and type (if multiple types are supported);

b) Liability Report. The liability report shall include the previous days starting value of outstanding promotional liability, aggregate promotional in and out totals, expired promotional value, and ending promotional liability; and

c) Promotional Meter Reconciliation Summary and Detail Reports. These reports shall provide reconciliation of each participating gaming machine promotional meter(s) against the central system’s promotional activity.

16.13 Reserved for amendments

16.14 Modification of Critical Parameters

All changes to parameters that may impact promotion redemption frequency or amount, must be logged indicating:

a) who made the change;

b) the altered parameter;

c) the time and date of change;

d) the parameter value before and after the change; and

e) the reason for the parameter adjustment.

16.15 Prevention of Unauthorized Transactions

The following minimal controls shall be implemented by the central system to ensure that games are prevented from responding to commands for crediting outside of properly authorized promotional transactions (hacking):

a) The network hubs are secured (either in a locked/monitored room or area) and no access is allowed on any node without valid login and password;

b) The number of stations where critical promotional applications or associated databases could be accessed is limited;

c) The users who have the requisite permission levels/login to adjust critical parameters are limited; and

d) Procedures be in place on the system to identify and flag suspect player and employee accounts to prevent their unauthorized use to include:

i. Having a maximum number of incorrect PIN entries before account lockout;
ii. Flagging of "hot" accounts where cards (other instruments) have been stolen;
iii. Invalidating accounts and transferring all balances into a new account; and
iv. User roles or procedures are established in promotional parameter configuration applications, which enforce logical separation of controls to discourage obvious misbehavior.

16.16 Communication Requirements

All topics covered in this section are also subject to the standards set forth in **Section 6.00 "Communication"** of this document to ensure the highest level of integrity possible.

16.17 Full Transfer of all Transactions

If a player initiates a promotional transaction, and that transaction would exceed game configured limits (i.e. the credit limit, etc) then this transaction may be rejected because a partial transaction may never occur.

16.18-16.21 Reserved for amendments

16.22 Error Conditions

The following conditions must be monitored, and messages must be displayed to the patron, which would indicate the reason for any transaction failure to include the following:
a) Invalid PIN or Player ID (can prompt for re-entry up to maximum allowed);and
b) Account unknown.

16.23 Diagnostic Tests on a Promotional Gaming Device

Controls are placed on any diagnostic functionality available at the device/system such that all activity would reflect a specific account(s) and the individual(s) tasked to perform these diagnostics whereby all promotional diagnostic activity that effect the gaming machine associated meters may be audited by SLGA.

16.24 Central System Audit Trails

The central system shall have the ability to produce logs for all complete promotional transactions to include the same information required on gaming machine audit logs and capable of being filtered by:
a) machine number;
b) patron account; or
c) promotional identification.

16.25 Transaction Report

The player must be provided the ability to review a complete and comprehensive transaction report of all promotional transactions concluded, indicating each separate transaction with amount.

NOTE: This audit trail could be accessed on the gaming device via the card reader (or equivalent) or such information could be requested of the floor personnel who would process such requests via a query of the promotional system.

16.26 Player Accounts

For awards tied to a specific patron's account, a casino usually issues a patron a unique card and may require a personal identification number (PIN), in conjunction with an account on the central system's database, although any method of uniquely identifying patrons could be implemented. All such transactions between a supporting gaming machine and the central system must be secured either by card insertion into a card reader attached to the central system or other protected means. The promotional options are presented to the patron on the LCD/VFD display of the card reader, which should require selection using a keypad/touchscreen before occurring.

16.27 Removing Promotional Credits from a Players Account

Promotional credits may be removed from a player's account either through:
a) Downloading of the promotional credits to the gaming device;
b) Redeeming the promotional credits for merchandise/cash via a cashier; or
c) Expiration of promotional credits.

16.28 Movement of Promotional Credits

Players may have the option of moving some of their system promotional credit to the gaming device, they are playing, through "withdrawal" from the players account, maintained by the system. Then when they are finished playing they may either "deposit" their balance from the machine onto their player account or redeem them from the gaming device via the available payout mechanism. Promotional gaming transactions are entirely electronic.

16.29 Personal Identification Number

Usually a casino issues a patron a unique magnetic card and personal identification number (PIN) in conjunction with an account on the system's database, although any method of uniquely identifying patrons could be implemented.
NOTE: Security of this information must be guaranteed at all times.

16.30 Account Balance

Current balance information and promotional award transaction activities should be available on demand at any participating gaming device or other system terminal after confirmation of patron identity. All discretionary account funds (i.e. those funds that have a possible expiration) must be maintained separately.
NOTE: Security of this information must be guaranteed at all times.

17.00 Definitions

Access Method – A method of security permitting specific, individual users to gain access to applications based on user privileges and levels. Access method is usually in the form of a personal identification number (PIN) or a password.

Algorithm – A step-by-step problem-solving procedure, especially an established, recursive computational procedure for solving a problem in a finite number of steps.

Audit Trail – A type of "log" that records specific information. Usually associated with computer applications to record access into systems, dates, times, changes. A method of implementing

security for databases or other sensitive programming. See an '***Event Log'*** for an example of an audit trail.

Bonusing Systems - Are comprised of gaming devices that are configured to participate in electronically communicated bonus award payments from a central system, and the central system that controls the bonus award issuance parameters. Bonus awards are those based on a gaming machine event or some external trigger which do not include triggers based upon specific patron activity

Cashless System – A cashless system is a central system that utilizes technology to allow players the ability to upload, download, transfer and redeem credits or cash independently on the gaming floor via other gaming devices and kiosks. The ultimate apex of a cashless system is, through the use of a medium such as a player card or debit card, eliminate the need for physical cash to be handled by the player or casino staff.

Central system – Monitoring and control systems, otherwise referred to a '*Central System*' or '*Central Accounting System*' or '*Host System*' or '*On-Line System.*

Critical Data – Information that is significant and is proprietary to either the operator or the customer that may compromise integrity of the organization or individual if it fell into the hands of an unauthorized individual or organization. Types of information that would be considered critical are: personal banking information, private information, social insurance numbers, executable computer code for operating systems, confidential corporate records or transactions.

CSA – Acronym for Canadian Standards Association.

Data Collector – An intermediate interface device used to gather information and data from a connected electronic gaming device and relay the information to the central system

Delta Function – Terminology used to describe a method by which accounting meters are calculated by subtracting new, or updated meters from previous meters. The difference represents the meter amount used for accounting purposes.

Downwardly Compatible – Usually in reference of different versions of software. Downwardly compatible means that, in reference to itself, it is compatible with earlier versions of software that the newer software design is based on. It is implied that this "newer" version of software will integrate seamlessly with older versions with little to no disruption of application features. Thus permitting older versions to not become obsolete

EGD – Acronym for electronic gaming device pursuant to Section 198 of *The Canadian Criminal Code.*

Event Log – A continuous digest of real-time information being passed along from the data collectors to the central system. Typical events recorded are:

- Main door open;
- electronic gaming device off line;
- Reel errors;
- Battery low errors; and

- Any code initiated by the EGM to describe any event occurring to the unit.

FEP – Front end processor. A computer that is dedicated to managing data communications

Firewall – Any of a number of security schemes that prevent unauthorized users from gaining access to a computer network or that monitor transfers of information to and from the network.

Flag – For the purposes of this document, the term "flag" shall mean a security event or notification sent to the central system.

Flash – A form of memory for computer code that is typically non-permanent. This can be updated via communications interface.

Flashable – A description of the "style" of memory device, or a verb used to describe the method of changing or updating memory

Hold Percentage – The percentage that represents the amount withheld by the gaming device during play. The value is calculated as follows: **100%- Payout Percentage**. Can represent either "*theoretical*" or "*actual*," depending on which type of "*Payout Percentage*" is used in the calculation.

Kiosk – A self contained redemption center used by players to independently redeem coin and coupons in exchange for cash value. A kiosk is linked to a central system to validate cash out tickets, has a self contained coin dispenser and bill dispenser to accommodate the transaction.

LCD – Acronym for liquid crystal display.

LED – Acronym for light emitting diode

Multi-Denomination – Similar in concept to "tokenization." However, it is not dependent on a base value, or the intrinsic value of the coin or note inserted into the gaming device to accumulate credits. Rather, a customer can choose what base value is preferred and played based on personal choice.

Mystery Progressive – Casino term for a type of secondary prize available to players on gaming devices where each device participating in the mystery progressive contributes to a total prize amount. Payout of the prize IS NOT dependent on a particular winning combination of a specific gaming device that is linked to the bonus prize amount.

Noise – Technical speak for a form of electronic interference. Usually associated with communication networks causing errors or inhibiting communication.

Non-Volatile – A term describing a storage device whose contents are preserved when its power is off. A form of memory that typically has battery back up in the event of power loss.

Payout Percentage (***Actual***)– The mathematical value correlating to total credits played vs. total credits won where winnings are divided by amount played. This relationship is expressed as: **(Credits Won + Jackpots) / Credits Played**. Referred to as "actual" because the value is

representative of the actual payout percentage of the machine at the time of calculation. (See *Payout Percentage (Theoretical*)" for comparison.)

Payout Percentage (Theoretical) – The payout percentage as calculated by a gaming device manufacturer to describe the anticipated, or expected, future payout percentage of the gaming device. (Sometimes referred to as: "*Target Percentage*.")

PIN – Acronym for Personal identification number

Private-Key encryption – An encryption key that is known only to your computer.

Progressive – Casino term for a type of secondary prize available to players on gaming devices where each device contributes to a total prize amount on top of a base value usually initialized by a casino. Payout of the prize is dependent of a particular winning combination on a specific gaming device that is linked to the progressive.

Promotional System – A promotional system is similar to both a bonus system and a cashless system. The difference being that a promotional system will transfer credits of approximately equal value to promotional items available as prizes. This method is typically used by American casinos as a method of circumventing tax laws for both casinos and customers.

Protocol – Computer speak for rules determining the format and transmission of data from one electronic device to another.

PSD - Acronym for "Program Storage Device." A generic term to encompass all forms of memory media known and unknown used by the Gaming Industry. Examples of which are: CDROM's, Hard Drives, EPROM's, flash RAM, etc..

Public-key encryption - A combination of a private key and a public key. The public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key.

RAM – Random Access Memory

RNG – Random Number Generator. The fundamental basis for gaming device technology

SAS – An acronym developed by International Gaming Technology used to describe a type of communications protocol.

Secure Protocol – These are the MINIMUM acceptable requirements necessary for establishing 'secure protocol.' Methods usually include: encryption, hashing algorithms, hardware encryption, etc…

Seeding – For the purpose of this document, the term "seeding" shall be used to describe the method of which random numbers are generated and used by the gaming device. "Seeding" is a technological term used to describe the placement of information.

Server – A computer which provides some service for other computers connected to it via a network.. The most common example is a file server which has a local disk and services requests from remote clients to read and write files on that disk. Typically a dedicated computer system to manage and direct the overall operation of a shared database.

Seven Segment Display – a collection of seven (7) LED's assembled in such a manner to illuminate as numerical digits.

Site Operator – Casino.

Tokenization – A configuration for gaming devices where the value of the coin, bill or token used on the gaming device does not correlate directly to an exact amount or face value amount that the individual coin, token, or bill is worth. An example: Nickel tokenization refers to a gaming device that will accept one quarter or token whose intrinsic value is 25 cents, but issue 5 credits available for play.

UL – Acronym for United Laboratories

Upwardly Compatible – Usually in reference to different versions of software. Upwardly compatible basically means that, in reference to itself, it is compatible with later versions of software that is based on it's original design. It is implied that this "older" version of software will integrate seamlessly with newer versions with little to no disruption of application features.

Verification – Casino specific term that describes the process of authenticating critical memory or programming.

VFD – Acronym for vacuum filled display.

18.00 Revision Log

REVISION #	DATE	SECTION CHANGED
001		
ORIGINAL LANGUAGE		
AMENDED LANGUAGE		
REVISION #	DATE	SECTION CHANGED
002		
ORIGINAL LANGUAGE		
AMENDED LANGUAGE		
REVISION #	DATE	SECTION CHANGED
003		
ORIGINAL LANGUAGE		
AMENDED LANGUAGE		
REVISION #	DATE	SECTION CHANGED
004		
ORIGINAL LANGUAGE		
AMENDED LANGUAGE		
REVISION #	DATE	SECTION CHANGED
005		
ORIGINAL LANGUAGE		
AMENDED LANGUAGE		
REVISION #	DATE	SECTION CHANGED
006		
ORIGINAL LANGUAGE		
AMENDED LANGUAGE		