INTEGRITY CERTIFICATION REQUIREMENTS:
CENTRAL SYSTEMS FOR VIDEO LOTTERY TERMINALS

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 video lottery terminals in Saskatchewan.

Background

These standards were developed in consultation with Western Canada Lottery Corporation, and SLGA Gaming Operations Division. Additionally, documents on central systems for Video Lottery Terminals were consulted including: Gaming Laboratories Incorporated (Standard Series 16,18,20, Version 1.3, November 10th, 2000); Nevada Gaming Control Board (Technical Standards for Slots, January 15, 1999), West Virginia (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.

1.0 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, suppliers, 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 video lottery terminals, covering: hardware, software and data base requirements, system communication, reporting, security requirements, program verification, and ticket validation.

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 by 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;
   - Include maintenance schedules outlining the elements of the central system that require maintenance, and the frequency at which that maintenance should be carried out; and
   - Include maintenance checklist that enable appropriate staff to make a record of the work performed and the results of the inspection.
   - 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.

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

2.00 Site Controller Hardware and Software Requirements

2.01 Reserved for Amendments

2.02 Design

The site controller shall be designed and manufactured robustly enough to withstand a typical environment of a bar or tavern setting. Environmental conditions to consider would be frequent spills, smoke, bumping, potential physical abuse.

When subjected to ESD, devices must not interfere with the operation of any other attached devices via local data communications cabling.

If the supply of main power to a device is disrupted, the device must not interfere with the operation of any other attached device via local data communications cabling.

2.03 Modularity

The site controller shall be designed and manufactured in such a manner to permit ease of replacement. There shall be no "hard wiring" required. Rather, a system of "quick-connects" or plugs shall be used.

2.04 Minimum Machines

The site controller shall be manufactured to support up to a minimum of 12 VLTs.

2.05 Types

The site controller shall be manufactured to support a variety of VLTs manufactured by different companies with the understanding that the VLTs will adhere to the communications protocol employed

2.06 Reserved for Amendments

2.07 Reporting

The site controller shall support reporting requirements outlined by SLGA.

2.08 Synchronization

The site controller shall permit synchronization of time and date with the host central system.

2.09 Diagnostics

The site controller shall have designed within the software specific tests that can be initiated by technical staff for the purposes of real-time diagnostics of the site controller and associated VLT communications.

2.10 – 2.16 Reserved for Amendments

2.17 Access

The site controller must log and report to the central system the following:
a) Site controller identification;

b) Operator;
c) Date and time of access at sign on; and
d) Date and time of access at sign off.

2.18 Password Protection

The site controller must provide separate password-protected access to authorized crown agent, and retailer.

2.19 Internal Logic

The site controller must have "internal sanity logic" to ensure the validity of data and operation

2.20 Generation and Validation of Tickets

Generation and validation of tickets must be secure, complete and accurate. The validation system or central system must have the ability to identify these occurrences and notify the central system 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).

Refer to section '5.00 Communication' and '13.07 Invalid Ticket Notification' for further details.

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 Site Controller Requirements

A central system may possess front end processors that gather and relay all data from the connected site controllers to the associated database(s). The site controllers, in turn, collect all data from connected VLTs. Communication between components must 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: (this includes site controllers)

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of 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 central system components. All internal clocks shall be synchronized by the central system, including the site controller, and the VLT.

3.07 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 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 site controller/VLT identification number; and
c) Significant event number(s).

3.08 Access

The central system must be capable of providing SLGA "read only" access to the data and all reporting functions at all times.

4.00 Database Requirements

4.01 Management Functionality

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

4.02 Parameters

The central system shall maintain the following information for VLT associated with the central system:
a) Unique serial number/CPU number (*or other, unique designation*) of the VLT;
b) VLT identification number as assigned by the province of Saskatchewan or it's agent;
c) Location;
d) Device description;
e) Game name or theme; and
f) Configuration;
    i. Denomination;
    ii. Software version/ control program(s) within VLT; and
    iii. Theoretical payout percentage of the VLT.

4.03 Database Access

The central system shall have no built-in facility whereby the site contractor can bypass system auditing to modify the database directly. The province of Saskatchewan, or it's approved agent 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.

4.04 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 the 9.01 Reporting Requirements,' as well as all internal control required reports.

4.05 Vital Transactions

The VLT Central System must be designed to provide the complete recovery of the database and central system functionality with near zero (0) data loss within a reasonable period of time, subject to the review and approval of SLGA, or its Agent.

5.00 Communication

5.01 Due Diligence

It is the responsibility of the manufacturer to ensure that the central system be designed to be as impervious to communication disruption as possible. 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.

5.02 General

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;

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; and

c) If the system permits the use of bi-directional communication, the necessary security measures shall be employed.

5.03 Hierarchy

For informational purposes, the manufacturer must provide documentation to SLGA outlining the communications methodology and provide all relevant protocol specifications employed by the central system.

5.04 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 at least at the lowest level of the protocol;

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.

5.05 Bi-Directional Requirements

Significant emphasis shall be placed on the integrity of the communication system for bi-directional data. VLT 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; and

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 the SLGA.

5.06 Encryption

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.

5.07 Technical

The VLT and site controller shall have the capability of visually indicating the status of communications to and (Tx/Rx host) from the central system (site controller) and to and from (Tx/Rx) VLT. This can be achieved through the use of a diagnostic selection on the

VLT and site controller whereby the activity can be viewed on the monitor, LED's or a seven segment display, through other recognized diagnostic methods.

It is up to the gaming laboratory to determine if the manufacturer has provided the adequate means of achieving this, and can be approved on a case by case basis if necessary by SLGA.

6.00 System Functionality

6.01 Requirements

The central system must have the ability to perform the following:

a) The ability to configure VLTs;
b) The ability to enable/disable VLTs;
c) The ability to retrieve a "snap shot" of information as it pertains financial, and game play on a specific VLT;
d) The ability to retrieve security data from a specific VLT; and
e) The ability to solicit an internal "self test" from an individual VLT or group of devices which will report the state of internal components.

6.02 Wireless Technology

6.02.1 Non-critical applications

"Non-critical" applications for use of wireless technology have not been identified for video lottery systems, and as such, are not allowed.

6.02.2 Critical applications

Wireless technology is not allowed for use to transmit or receive any information that pertains to credits, Personal identificationnNumber (PIN), player tracking, 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.

7.00 Events

7.01 Event Format

Events are generated by a VLT and sent via the site controller 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 VLT that generated the event;
c) A unique code that defines the event; and
d) A brief text that describes the event.

7.02 Handling of Critical Fault of VLT

The central system must have the capability to facilitate a prompt reporting of faults that would require a manual re-activation.

7.03 Standard Events

The following significant events must be collected from the VLT and transmitted to the system for storage:

a) Power resets or power failure;
b) System administration events;
c) Transaction information including:
    i Machine number;
    ii. Date and time (24hr format);
    iii. Ticket sequence number;
    iv. Validation number;
    v. Bar code or any machine readable code representing the validation number;
    vi.Type of transaction or other method or differentiating ticket types; and
    vii. Indication of an expiration period from date of issue, or date and time the ticket will expire (24 hr. format).
d) Bill (item) Acceptor Errors including:
    i. Stacker full (if supported); and
    ii. Bill (note) jam.
e) VLT Low RAM battery error;
f) VLT RAM reset;
g) Hard meter faults;

7.04 Priority Events

The following significant events must be conveyed to the central system where a mechanism must exist for **timely notification**:

a) Loss of communication with site controller;
b) Loss of communication with VLT;
c) Memory corruption of the site controller;
d) RAM corruption of the VLT;
e) Any external door openings on the VLT;
f) Catastrophic software corruption;
g) Unrecoverable hardware faults;
h) Game EPROM/program mismatch; and
i) Signature check failure.

8.00 Meters

8.01 Information

Metering information is generated on a VLT and collected by the site controller and sent to the central system via a communication protocol. This information may be either read directly from the VLT 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 metering information must be communicated from the VLT:

a) Total In (credits-in);
b) Total Out (credits-out);

c) Credits Played;
d) Credits Won;
e) Bills In (total monetary value of all bills accepted);
f) Items In (total value of all items accepted);
g) Individual Bill Meters (total number of each bill accepted per denomination);
h) Games-Played;
i) Cabinet Door (instance meter which may be based on central system count of this event);
j) Cash Door(s) (instance meter which may be based on central system count of this event); and
k) (Optional) Progressive (or Jackpot instance meter shall count the number of times progressive meter is activated).

NOTE: Please refer to the SLGA standards for VLTs, **Sections: 2.45 Electronic Accounting and Occurrence Meters, 2.43 Progressives, 1.20 Hard Meters**. While these electronic accounting meters should be communicated directly from the VLT to the central system, it is acceptable to use secondary central system calculations where appropriate.

8.03 Hard Meters

The VLT shall maintain non-resetable, electromechanical meters to capture, at a minimum, the following information:
a) Total In (credits-in);
b) Total Out (credits-out);
c) Credits Played; and
d) Credits Won.

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 the 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 VLT;
b) Monthly VLT revenue summary;
c) Theoretical hold vs. actual hold comparison with variances;
d) Significant event log for each VLT;
e) A network topology report;
f) A network status report;
g) Anomolies report;
h) Meter checking report;
i) Adjustment report; and
j) Net win for entire system.

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.

10.02 Design

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

10.03 Software Management

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.

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.

10.04 Audit Log

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) What data was affected; and
vi) The original data.

10.05 Personal Identification Number (PIN) Management

If a PIN is used in any manner within VLT and/or the support system, the PIN creation algorithm and operational procedures (i.e. PIN changes, database storage, security and distribution) must all be approved. The storage of the PINs must be in an encrypted, non-reversible form. This means that if a person (authorized or not) 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.

10.06 System Upgrades and Modifications

The appointed agent or crown corporation is 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.

10.07 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 reasonable checks to verify the integrity of system processing, and using control totals on reports for comparison to input figures.

10.08 Data Alteration

The central system shall not permit the alteration of any accounting or significant event log information that was properly communicated from the VLT 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).

10.09 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 removal of the information unless it has first transferred that information to the database or other secured component(s) of the validation system. See Section 4.00 ‘DATABASE REQUIREMENTS’ for further information.

11.00 VLT Program Verification Requirements

11.01 Verification

A central system must provide program verification functionality to check VLT game 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).

11.02 Verification Algorithm Timing

Verification may be user initiated or triggered by specific significant event(s) on the VLT. To ensure complete coverage, verification should be performed, at a minimum, after each of the following events:
a) VLT Power Up; and
b) New VLT installed.

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

11.03 Signature Calculations Mandatory

Software signatures must be calculated on all VLTs at all venues and are to be validated by the site controller/central system network.

11.04 Minimum Signature Algorithm Requirements

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 least 16-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.

11.05 Signature Seeding

a) Signature algorithm "seeds" (also known as "algorithm coefficients") 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 least 16 bits in length; and

ii. The "seed" information is to influence the behavior of the algorithm in a non-trivial way.

11.06 Signature Calculation Requirements

a) If the normal signature check of the entire program exceeds ten (10) seconds, a strategy of an immediate signature check of the VLT plus a background signature check of the entire program range when signatures are required, may be approved. Approval is contingent upon the testing laboratory ensuring the method is viable and accurate.

b) A signature check of the entire range of the program must be performed for VLT or site controllers when any of the following events happen:

i. The signature seed set is changed at the site controller/central system;
ii. New firmware (programming) is installed in the VLT;
iii. New software is downloaded to the VLT;
iv. A VLT 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;
v. A RAM reset has occurred; or
vi. The logic area cabinet door has been shut (after being opened).

c) Additional to the situations listed above, all VLTs with PSD's (i.e. VLT with storage mediums that support program data downloading) must have central system initiated signature validations scheduled at least once (1) per day.

12.00 Additional System Requirements

12.01 Memory Capacity

The central system shall be equipped with the appropriate amount of memory to adequately handle all database requirements and operational requirements necessary to operate.

12.02 System Scalability

Software. The system must be designed such that it readily accepts software enhancements without requiring a complete redesign of existing software. The software must be both "upwardly" and "downwardly" compatible.

Hardware. Upgrades must not require software application conversions or upgrades

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.

12.03 Downloadable, Re-writable Software Requirements

If supported, a central system may utilize FLASH (or similarly equivalent) technology to update the site controller software if all of the following requirements are met and are subject to the conditions set for in Section‘11.00 VLT 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 the version(s) of code that 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 the flash file(s) that can be verified by SLGA 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.

12.04 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, and 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) 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.

12.05 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 VLTs 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.

12.06 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:
a) Significant events;
b) Accounting information;
c) Auditing information; and
d) Specific site information such as VLT file, set-up, etc.

The optimal recovery method from a hard drive failure is to have software that is capable of automatically rebuilding.

13.00 Ticket Validation

13.01 Validation

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

13.02 Payment by Ticket Printer

Payment by ticket printer as a method of credit redemption on a VLT is only permissible when the VLT 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.

13.03 Ticket Information

A ticket shall contain the following printed information at a minimum:

a) The name ‘Saskatchewan’;
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)

13.04 Ticket Issuance

A ticket can be generated at a VLT through an internal document printer, at a player’s request, by redeeming all credits.

13.05 Reserved for Amendments

13.06 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; and
d) Amount.

13.07 Invalid Ticket Notification

The validation system or central system must have the ability to identify these occurrences and notify bar staff/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).

13.08 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 VLT; or use of an approved alternative method as designated by the regulatory jurisdiction that will accomplish the same.

13.09 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) Transaction detail report must be available from the validation system that shows all tickets generated by a VLT and all tickets redeemed by the validation terminal or other VLT.

14.00 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.

ARQ **-** Automatic Repeat Request.

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.

Central system – Monitoring and control systems (…otherwise referred to a '*central system*' or '*central accounting system*' or '*host system*' or '*on-line system'*…)

Checksum **-** A software process whereby the entire contents of a program or file are run through a mathematic equation or algorithm (in binary format) to produce an 8-bit or 16-bit binary result.

Concatenation **-** A sequential summation of two (2) things (e.g. the concatenation of 24, 0297, and 455 is 240297455).

CRC **-** Cyclic Redundancy Check. A CRC is a method for checking the accuracy of a package of data. For communications applications: A CRC is a method for checking the accuracy of a digital transmission over a communications link. The sending computer performs a calculation on the data and attaches the resulting value. The receiving computer performs the same calculation and compares its result to the original value. If they do not match, a transmission error has occurred and the receiving computer requests a retransmission of the data. For data storage applications, a CRC is a method for checking the validity of a digital file. The validating computer performs a calculation on the data within the digital file and compares the resulting value to a previously recorded (correct) value. If they do not match, the contents of the digital file must have somehow been altered.

Critical Data – Information that is significant and is proprietary to either the operator or the customer that may compromise integrity of the organization or the 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, and confidential corporate records or transactions.

CSA – Canadian Standards Association.

Data Collector – An intermediate site controller used to gather information and data from a connected VLT and relay the information to the central system.

Downwardly Compatible – Usually in reference of different versions of software. Downwardly compatible basically 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.

ESD – Acronym for 'electro-static dishcarge'

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;
- VLT off line;
- Reel errors;
- Battery low errors; and
- Any code initiated by the EGM to describe any event occurring to the unit.

Exclusive-OR Arithmetic - The contents of the accumulator are exclusive-ORed, bit by bit, with the contents of the addressed core-storage location. The result replaces the contents of the accumulator. Exclusive-ORing occurs only between corresponding bit positions in the accumulator and the core-storage word: bit 0 is exclusive-ORed only with bit 0, bit 1 only with bit 1, and so on.

FEP – Front End Processor. A computer that is dedicated to managing data communications.

Firewall – Any of a number of software security schemes that prevent unauthorized users from gaining access to a computer 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.

Foreground Signature Check - A foreground signature check is a method of verifying the vital/critical contents of a system's programming.

Interrupt – Computer programming definition used to describe a method by which peripheral devices interacts with the processing routine of a microprocessor, or central processor.

ISO - International Standards Organization.

LAN - A local network for inter-computer communication; especially a network connecting computers to create an inter-site system.

LCD – Liquid Crystal Display.

LED – Light Emitting Diode.

Meter Wrapping – The term used to describe the situation when a meter exceeds its upper limit and returns to zero, thus creating a negative difference between the previous value and the current value.

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 VLT to accumulate credits. Rather, a customer can choose what base value is preferred and played based on personal choice.

NAK - Negative Acknowledgement.

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.

Parity **-** A parity check is a software process whereby the entire contents of a program or file are run through a logical process (in binary format) to produce a 1-bit binary result (either a one (1) or a zero (0)).

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 / 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 VLT manufacturer to describe the anticipated, or expected, future payout percentage of the VLT. (Sometimes referred to as: "*target percentage*.")

PCB – Printed Circuit Board.

Progressive Jackpots **-** For the purposes of this document, a progressive jackpot is an award for a winning or non-winning (e.g. mystery jackpot) play of the game.

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

PSD - Program Storage Device. A form of memory media.

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

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.

PSTN – Public Switched Telephone Network.

RAM – Random Access Memory.

RNG – Random Number Generator. The fundamental basis for VLT technology

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 VLT. "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.

Site Controller – A device used for the purposes of communicating with a LAN of VLTs at a specific site. It governs communication between the VLTs and is responsible for maintaining communication with the central system through the use of a “dial up modem” or a “leased line” carrier.

Site Contractor – SLGA approved licensed establishment who has agreed to the terms and conditions outlined in the “VLT Site Contractor Agreement.”

Software Suite - A versatile, fully integrated, multi-faceted conglomeration of programs or programming to create a cohesive package known as a “suite.”

ULC – 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.

VFD – Vacuum Filled Display.

VLT – Video Lottery Terminal.

VMT – see ‘Site Controller’.

WAN - A communications network that uses such devices as telephone lines, satellite dishes, or radio waves to span a larger geographic area than can be covered by a LAN.

15.00 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		