INTEGRITY CERTIFICATION REQUIREMENTS

Electronic Raffle Systems

Saskatchewan Liquor and Gaming Authority

January 2018

Table of Contents

Revision History

REVISION APPROVAL DATE	REVISION DESCRIPTION	REVISION TRACKING NOTES
January 2018	Merged and reorganized two previously approved standards regarding raffle systems: 1. Online Raffle Sales Standards, 2014 2. Integrity Certification Requirements - Electronic Raffle Systems, 2016	All sections from both documents have been incorporated into a single standard.

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*. This document outlines the integrity certification requirements for Electronic Raffle Systems (ERS). All systems used for Venue-Based sales, online sales, the management and auditing of raffle tickets, and for the use of Random Number Generators (RNGs) must meet the requirements contained within this document and any relevant charitable gaming Terms and Conditions set forth by SLGA.

Background

These standards were developed from consultations with Gaming Laboratories International, LLC, Burnaby, British Columbia, referencing GLI standards: GLI-26 Wireless Systems v2.0, February 24, 2015; GLI-27 Network Security Best Practices v1.1, January 21, 2013; and GLI-31 ERS , v.1.1, July 24, 2015, Trusted Geolocation in the Cloud: Proof of Concept Implementation (NISTIR 7904), National Institute of Standards and Technology, U.S. Department of Commerce, International Organization for Standardization, Information Systems (ISO), ISO 27001 and 31000 Series and Control Objectives for Information and Related Technologies (COBIT), COBIT 5.

Purpose

These standards are intended to provide regulatory guidance to manufacturers, suppliers and gaming operators and licensees regarding technical gaming integrity requirements in Saskatchewan. Where variations from these standards are proposed, SLGA 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.

IN.1.00 General

IN.1.01 Ownership and Control of Technical Gaming Integrity Document

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

IN.1.02 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.

IN.1.03 Parameters of Document

This document outlines those requirements that apply to ERS to create a standard which will ensure that ERS are fair, secure and have the capability to be audited and operated in accordance with SLGA as the regulator.

IN.1.04 Technology

SLGA recognizes that technology changes. New technology will be evaluated, as required, and the standards amended accordingly.

IN.2.00 Regulatory Requirements

IN.2.01 General

SLGA reserves the right to decide what constitutes an ERS and determine what type of product requires laboratory testing.

All ERS must be tested by an independent test laboratory approved by SLGA to meet the applicable requirements set forth in this document. For circumstances where there is uncertainty regarding specific testing requirements, SLGA will review each situation and engage in discussions with the testing laboratory and manufacturer to make a determination.

IN.2.02 Asset Management

All assets housing, processing or communicating controlled information, including those comprising the operating environment of the ERS and/or its components shall be:

a) Accounted for and have a designated "owner" responsible for ensuring that information and assets are appropriately classified, and defining and periodically reviewing access restrictions and classifications;
b) Housed in a secure, controlled location such that access to the ERS is limited to authorized personnel; and,
c) Physically located within the boundaries of the Province of Saskatchewan.

IN.2.03 Software Updates

Changes to the systems that would affect the critical files are not permitted without first consulting SLGA. If a manufacturer proposes to makes changes to the system that substantially affects system software, the manufacturer will be required to submit the change to an approved laboratory for testing prior to implementation in the field. SLGA reserves the right to determine what constitutes a substantial change. SLGA shall be notified of any system updates or changes and may request additional information regarding the specific system components that may be affected. As well, SLGA may request a report from the manufacturer identifying:

a) The nature of the software change(s);
b) The modules affected by the change(s); and
c) Proposed date of change.

IN.2.04 Network Security Management

To ensure security of ticket purchaser privacy, security requirements shall apply to the following critical components of the ERS:

a) ERS components which record, store, process, share, transmit or retrieve sensitive purchaser or payment information, e.g. credit card/debit card details, authentication information, purchaser account balances, online payments;
b) ERS components which store results of the current state of a purchaser's order or payment;
c) Points of entry to and exit from other systems which are able to communicate directly with the core critical systems; and
d) Communication networks which transmit sensitive purchaser information, e.g. payment gateways.

IN.2.05 Information Systems Security (ISS) Industry Standards

SLGA specifies the requirements for establishing, implementing, maintaining and continually improving information security management processes within the context of any products

submitted for testing. Furthermore, aspects of products that fall outside the realm of testing by the laboratory are subject to assessment and treatment of information security risks tailored to the design and functionality of the product. These subsequent requirements set out by SLGA are generic and are intended to be guiding principles to all gaming system related products, regardless of type, size or nature.

IN.2.06 Normative references

The following documents, in whole or in part, are normatively referenced by SLGA and are indispensable for implementation or deployment of gaming system products:

a) International Organization for Standardization, Information Systems (ISO), ISO 27001 Series;
b) International Organization for Standardization, Risk Management, ISO 31000 Series:
c) Control Objectives for Information and Related Technologies (COBIT), COBIT 5;
d) Payment Card Industry (PCI), PCI Data Security Standard v3.2.

This list is not exhaustive and should not be interpreted as the only source of guidance. Other normative references will be considered on by SLGA a case-by-case basis.

IN.2.07 Manuals

Technical and operational information must be directly relevant to system being submitted for testing and must be provided at the request of SLGA. Required information may include:

a) Operational manuals associated with the applicable system;
b) Technical Service manuals which:
    i. Accurately depict the system for which the manual is intended to cover;
    ii. Provide adequate detail and are clear in their wording and diagrams to support interpretation by SLGA personnel;
    iii. Include a maintenance schedule outlining the elements of the system that require maintenance and the frequency at which that maintenance should be carried out;
    iv. Include a maintenance checklist that enables appropriate staff to make a record of the work performed and the results of the inspection; and
    v. Include a complete list and samples of available reports that can be generated by the system.
a) Technical documentation that provides adequate detail and is sufficiently clear in wording and diagrams to enable a review/evaluation of the system used;
b) Complete documentation for programming patches, fixes and any upgrades made to the system.

Part I
1.0.00 Common Requirements

1.1.01 General
The criteria set forth within this section provide the foundation for any type of ERS and are common to all test submissions. Depending on the type of ERS submitted for testing, specific criteria applicable to a particular product can be located in subsequent sections of this document. The testing laboratory or SLGA will clarify instances of ambiguity regarding the application of requirements.

1.1.02 Access Control
The ERS must be logically secured and protected against intrusion and unauthorized access. These protective methods may include:

a) Passwords;
b) PINs (Personal Identification Numbers);
c) Security Access Levels dependent on different classes of administrative responsibilities;
d) System administrator notification and user lockout or audit trail entry, after a set number of failed login attempts; and,
e) Any other methods deemed acceptable by SLGA.

1.1.03 Remote Access
The manufacturer/supplier may be required to remotely access the system and its associated components for the purpose of product and user support. Remote access is defined as any access from outside the system or system network including any access from other networks within the same establishment. Remote access shall remain disabled and be allowed only if authorized by SLGA. The manufacturer shall have no access:

a) To administration functionality (i.e. adding users, changing permissions, etc.);
b) To any database other than information retrieval using existing functions;
c) To the operating system; and
d) During the operation of a "live" raffle.
e) Any exceptions will be determined by SLGA on a case-by-case basis.
f) The ERS must maintain an activity log which updates automatically depicting all remote access information to include:
    i Log-on name;
    ii Time and date the connection was made;
    iii Duration of connection; and
    iv Activity while logged in, including the specific areas accessed and the changes that were made.

1.1.04 Security from Tampering or Unauthorized Access
Securing raffle data against alteration, tampering or unauthorized access is paramount and the ERS must provide a logical means for securing raffle data:

a) No equipment will have a mechanism whereby an error will cause the raffle data to automatically clear;
b) Data shall be maintained at all times whether or not server is supplied with power; and

c) Data shall be stored in such a way as to prevent the loss of the data when replacing parts or modules during normal maintenance.

1.1.05 Data Alteration

The ERS must not permit the alteration of any accounting, reporting or significant event data without access level permission. In the event that any data is changed, the following information must be documented or logged:

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) User that performed alteration (user login).

1.1.06 Backups, and Recovery

The ERS must properly back up critical information with the capability for timely recovery. The ERS shall have redundancy and modularity so that if any single component or part of a component fails, the raffle can continue. Redundant copies of critical data shall be kept with open support for backups and restoration. Storage must meet the following criteria:

a) The online system must properly back up critical information with a proven methodology for real-time recovery striving for zero downtime or loss of fidelity. The online system shall have redundancy so that if a failure occurs, transactions can continue.
b) All storage shall be through an error checking, non-volatile physical medium or an equivalent architectural implementation, so that should the primary storage medium fail, the functions of the ERS and the process of auditing those functions can continue with no critical data loss;
c) The database shall be stored on redundant media so that no single failure of any portion of the system would cause the loss or corruption of data.
d) If a system failure should occur, all processes and transactions shall be seamless and un-noticeable to the end-user.

1.1.07 Shutdown

The ERS must have the following capabilities:

a) The ERS must be able to perform a graceful shutdown with no loss of data and only allowing automatic restart after the following minimum requirements have been met on power up:
    i. Program resumption routine(s), including self-tests that complete successfully;
    ii. All critical control program components of the ERS have been authenticated; and
    iii. Communication with all ERS components have been established and authenticated;
a) The ERS must be able to identify any master resets that have occurred on system components;
b) The ERS must have the ability to recover all critical information from the last backup; and
c) If a system failure should occur, all critical information from the time of the last backup to the point in time that the system failure occurred must be recoverable.

1.1.08 Error Recovery

Messages received in error must be fully recoverable by the ERS. This would include inaccurately inputting personal/banking information which would result in the Purchaser being notified that the information is invalid and must require review and corrective measures. In the event of a catastrophic failure when the system cannot be restarted in any other way, it shall be possible to reload the system information from the last viable backup point and fully recover the contents of that backup, including, but not limited to:

a) Significant events;
b) Accounting information;
c) Reporting information; and
d) Specific site information such as employee file, raffle set-up, etc.

1.1.09 Recovery Requirements

In the event of a catastrophic failure when the ERS cannot be restarted in any other way, it must be possible to reload the ERS from the last viable backup point and fully recover the contents of that backup, including but not limited to:

a) Significant events;
b) Accounting information;
c) Reporting information; and
d) Specific site information such as employee file, raffle set-up, etc.

1.1.10 Firewalls

All connections to ERS hosts, including remote access, must pass through at least one application-level firewall and must not have a facility that allows for an alternate network path. This includes connections to and from any non-related hosts used by the operator. Any path existing for backup purposes must also pass through at least one application-level firewall.

1.1.11 Firewall Audit Logs

The firewall application must maintain an audit log and must disable all communications and generate a significant event if the audit log becomes full. Logs shall be kept for a minimum of 90 days. The audit log shall contain:

a) All changes to configuration of the firewall;
b) All successful and unsuccessful connection attempts through the firewall; and
c) The source and destination IP addresses, and port numbers.

Note: A configurable parameter ‘unsuccessful connection attempts’ may be utilized to deny further connection requests should the predefined threshold be exceeded. The system administrator must also be notified.

1.1.12 System Clock Requirements

A system must maintain an internal clock that reflects the current date and time in twenty-four (24) hour format showing hours and minutes 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 sales and draw events.

1.2.00 Authentication

1.2.01 General

Systems and RSU's shall have the ability to allow for an independent integrity check of the components and modules from an outside source and is required for all software that may affect the integrity of the system

1.2.02 Authentication of Software and Devices

System software components, modules and RSU's shall be authenticated by a secure means at the system level denoting program ID and version. This must be accomplished by being authenticated by a third-party device or by allowing for removal of media such that it can be authenticated externally. Other methods may be evaluated on a case-by-case basis. This integrity check will provide a means for field authentication of the system components and modules to identify and validate programs and files. The independent test lab shall approve the integrity check method prior to system approval.

Part II
2.0.00 Online Raffle Tickets

2.1.00 Geolocation

2.1.01 Physical Location

The Online Raffle Ticket Sales system must be able to reasonably detect the physical location of an authorized Purchaser attempting to access the service. Third parties may be used to verify the location of Purchasers as allowed by the SLGA.

2.2.00 Tickets

2.2.01 Inventory

When issued a charitable gaming license to conduct a raffle, the charitable organization will specify the number of raffle tickets to be made available for sale through the Internet. The Online Raffle Ticket Sales system software is required to have the ability to set limits for the number of raffle tickets which may be purchased and the time over which tickets may be purchased. Online Raffle Ticket Sales must cease when the number of tickets allocated for online sales has been reached or when the time limit for online sales has been reached, whichever comes first.

2.3.00 Sales

2.3.01 General

Any system used for the sale of raffle ticket(s) through the Internet must have a device or facility that provides for the collection and accounting tools needed to determine all sales initiated through the Internet. The accounting information is subject to an operational and financial audit by SLGA.

2.3.02 Purchase Session

A purchase session consists of all activities and communications performed by a Purchaser during the time the Purchaser accesses the ERS/Online Purchasing Platform. Tickets can only be purchased during a purchase session.

2.3.03 Purchasing Tickets

A participant may purchase a raffle ticket from the website by following the instructions appearing on the screen and providing payment for the ticket(s). Each raffle ticket must be sold for the price indicated. Multiple discounted prices will only be allowed if a way of ensuring financial accountability is possible by the ERS:

a) A ticket purchase via a credit card transaction or other methods which can produce a sufficient audit trail must not be processed until such time as the funds are received from the issuer or the issuer provides an authorization number indicating that the purchase has been authorized;
b) There must be a clear notification that the purchase has been accepted by the system and the details of the actual purchase accepted must be provided to the Purchaser once the purchase is accepted; and
c) Purchase confirmation should include the amount of the purchase accepted by the Online ERS.

2.3.04 Disputes
There must be an easy and obvious mechanism available to advise the Purchaser of the right to make a complaint against the operator, and to enable the Purchaser to notify the SLGA of such a complaint.

2.3.05 Ticket Issuance
After the payment of a fee, the Purchaser shall receive a receipt through the Internet that the purchase of raffle ticket(s) is complete. Upon receiving the receipt acknowledging the raffle ticket(s) purchased through the Internet, the Purchaser can receive the raffle ticket(s) bought via e-mail.

2.3.06 Validation Numbers
The method used by the ERS to generate the ticket validation number must be unpredictable and ensure against duplicate validation numbers for the raffle currently in progress.

2.3.07 Official Draw Results
Results of the draw become official and final after the drawn number is verified as a winning raffle ticket. The winning draw number shall be made available through a website and/or through any other means of communication.

2.3.08 Voiding a Ticket
If a ticket is voided, the appropriate information shall be recorded, which includes the draw numbers and the validation number pertaining to the voided ticket. Voided draw numbers shall not be able to be resold or reissued.

2.4.00 Online Accounting Reports
2.4.01 Reports
Any system used for the sale of raffle ticket(s) through the Internet must have the capability to log sales and to print reports detailing sales and accounting information for specific dates and time periods must be available. This information must include, but is not limited to:

a) Data required to be maintained for each raffle drawing, including:
   i. Date and time of event;
   ii. Organization running the event;
   iii. Sales information;
   iv. Value of prize(s) awarded;
   v. Prize distribution;
   vi. Refund totals of event;
   vii. Draw numbers-in-play; and;
   viii. Winning number(s) drawn (including draw order, call time and claim status).

b) Exception Report. A report which includes system exception information, including, but not limited to, changes to system parameters, corrections, overrides and voids.

c) Ticket Reports. A report which includes a list of all tickets sold including all associated draw numbers and selling price.

d) Sales Report. A report which includes a breakdown of sales of raffle ticket(s) through the Internet, including draw numbers sold and any voided and misprinted tickets.

e) Event Log. A report which lists all events recorded specific to the sales of raffle ticket(s) through the Internet. This will include the date and time of the transaction and a brief description of the transaction and/or identifying code.
f) Corruption Log. A report which lists all Internet transactions that were unable to be reconciled to the system.
g) Sales and Accounting Report Requirements. Any raffle ticket(s) sold must be included in the sales and accounting reports and be detailed in all financial transactions on the system. In addition, a log relating to accounting and raffle ticket sales must be maintained on the system. The charitable organization conducting the raffle shall be given the option of printing this log on demand.

2.5.00 Online ERS Requirements

2.5.01 General

The following requirements are to be examined for Online ERS in addition to the requirements found in Part I.

2.5.02 Network Separation

Networks should be logically separated such that there should be no network traffic on a network link which cannot be serviced by hosts on that link.

a) The failure of any single item should not result in denial of service;
b) An Intrusion Detection System/Intrusion Prevention System must be installed on the network which can:
    i Listen to both internal and external communications;
    ii Detect or prevent Distributed Denial of Services (DDoS) attacks;
    iii Detect or prevent shellcode from traversing the network;
    iv Detect or prevent Address Resolution Protocol (ARP) spoofing; and
    v Detect other Man-in-the-Middle indicators and server communications immediately if detected.
c) All changes to network infrastructure (e.g. network device configuration) must be logged;
d) Virus scanners and/or detection programs should be installed on all pertinent information systems. These programs should be updated regularly to scan for new strains of viruses.

2.5.03 Communication Protocol

Online raffle ticket(s) offered for sale by a licensed charitable organization must support a defined communication protocol(s) that ensures purchaser(s) are not exposed to unnecessary security risks when using the Internet for this purpose. This includes utilizing the best security practices available at the time to the manufacturer. Each component of a ERS must function as indicated by the communication protocol implemented. The system must provide for the following:

a) All critical data communication shall be protocol based and/or incorporate an error detection and correction scheme to ensure accuracy of messages received;
b) All critical data communication shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication;
c) Communication between all system components must provide mutual authentication between the component and the server;

d) All protocols must use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent eavesdropping and tampering. Any alternative implementations are to be reviewed on a case-by-case basis, with regulatory approval;
e) All data communications critical to raffle ticket sales through the Internet shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication.

2.5.04 Bi-Directional Requirements

Significant emphasis shall be placed on the integrity of the communication system for bidirectional data. With the requirement of "two-way communication" where personal/banking information is transferred bi-directionally through a communication link, the security of the system is paramount. Any system used to sell raffle ticket(s) through the Internet shall 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 and personal identification numbers.

2.5.05 Cryptographic Controls

Cryptographic controls must be implemented for the protection of information.

a) Any sensitive or personally identifiable information should be encrypted if it traverses a network with a lower level of trust;
b) Data that is not required to be hidden but must be authenticated must use some form of message authentication technique;
c) Authentication must use a security certificate from an approved organization;
d) The grade of encryption used should be appropriate to the sensitivity of the data;
e) The use of encryption algorithms must be reviewed periodically by qualified management staff to verify that the current encryption algorithms are secure;
f) Changes to encryption algorithms to correct weaknesses must be implemented as soon as practical. If no such changes are available, the algorithm must be replaced; and
g) Encryption keys must not be stored without themselves being encrypted through a different encryption method and/or by using a different encryption key.

2.6.00 Online Purchaser Account Registrations

2.6.01 General

The Online ERS must employ a mechanism to collect (either online or via a manual procedure approved by the SLGA) purchaser information prior to registration of a purchaser account. The purchaser must be fully registered and their account must be activated prior to permitting ticket purchases.

2.6.02 Establishment of Purchaser Account

Once the identity verification is successfully complete, and the purchaser has acknowledged all of

the necessary privacy policies and the terms and conditions, the purchaser account registration is complete and the account can become active.

Part III
3.0.00 Random Number Generators

3.1.00 Requirements

3.1.01 General

An RNG used in Venue-Based ERS and Online Raffle Ticket Sales systems is defined as a computational device designed to generate a random number or sequence of numbers that lack any pattern. The approved RNG will reside on a Program Storage Device (PSD) that is contained in the server(s) used to operate the ERS. The number(s) selected by the RNG for each raffle draw must be stored in the system's memory and be capable of being output to produce a winning number(s). At a minimum, RNG requirements are:

a) All outcomes shall be available. All valid, sold raffle numbers must be available for random selection at the start of a raffle draw;
b) Protection of RNG. Appropriate communication protocols must be used by the ERS to protect the RNG and the random selection process from any outside influences (i.e. associated system equipment);
c) The RNG and random selection process must be impervious to influences from outside the ERS (i.e. electro-magnetic interference, electro-static interference, radio frequency interference, etc.).

3.1.02 Period

The period of the RNG, in conjunction with the methods of implementing the RNG outcomes, must be sufficiently large to ensure that all valid, sold numbers are available for random selection.

3.1.03 Range

The range of raw values produced by the RNG must be sufficiently large to provide adequate precision and flexibility when scaling.

3.1.04 RNG Requirements

The use of an RNG, in an ERS, results in the selection of a raffle outcome in which the selection must:

a) Be statistically independent;
b) Conform to the desired random distribution;
c) Pass various recognized statistical tests; and
d) Be unpredictable.

3.1.05 Applied RNG Tests

SLGA may employ the use of various recognized tests to determine whether or not the random values produced by the RNG pass the desired confidence level of 99%. The 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 test (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;
o) Poisson distribution; and
p) Any other tests deemed a requirement by SLGA.

3.1.06 Background RNG Activity Requirement

In order to ensure that RNG outcomes cannot be predicted, the RNG shall be cycled continuously at a speed that cannot be timed unless specifically designed to work "on demand." If an interruption is necessary and the RNG cannot be cycled, these exceptions shall be kept to a minimum.

3.1.07 RNG Seeding/Re-Seeding

RNG seeding/re-seeding must result in outcomes that are not predictable:

a) The first seed must be randomly determined by an uncontrolled event. If multiple draws have been approved, after every raffle ticket draw, there shall be a random change in the RNG process (i.e. new seed, random timer, etc.). This will verify that 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 the selection process will not synchronize.
b) Seeding and re-seeding must be kept to an absolute minimum.

3.1.08 Winning Number Draw

The winning raffle draw number shall be determined from the pool of sold raffle ticket numbers from the current raffle. If more than one (1) raffle draw is to occur during the time indicated on the licensee agreement, the winning number selection shall be produced only from sold raffle ticket numbers corresponding to the applicable raffle draw.

3.1.09 Scaling Algorithms

Scaling methods, converting raw RNG outcomes of a greater range into scaled RNG outcomes of a lesser range, must not introduce any patterns or be predictable.

a) If a random number with a range shorter than that provided by the RNG is required for some purpose within the ERS, the method of re-scaling, (i.e. converting the number to the lower range), is to be designed in such a way that all numbers within the lower range are equally probable;
b) If a particular random number selected is outside the range of equal distribution of re-scaling values, it is permissible to discard that random number and select the next in sequence for the purpose of re-scaling.

Part IV
4.0.00 Venue-Based Raffle Ticket Sales

4.1.00 Management

4.1.01 Prize Limitations

Software used in the Venue-Based ERS must be capable of being configured to set a limit on the maximum amount that may be won.

4.1.02 Time Limits

The Venue-Based ERS must have the ability to set time limits within which raffle tickets can be purchased for the raffle draw.

4.1.03 System Configuration Changes

Once a raffle has commenced, configuration settings for the raffle cannot be changed or altered until completion of the raffle.

4.2.00 Tickets

4.2.01 Raffle Sales Unit (RSU)-Generated Tickets

All tickets must, at a minimum, contain the following information, which is retained by the system:

a) Draw number(s) for each purchased ticket;
b) Value or cost of the ticket;
c) Date and time the ticket was issued in twenty-four (24) hour format showing hours and minutes;
d) RSU identifier from which the ticket was generated;
e) Unique validation number or barcode;
f) Name of licensee;
g) Licensee license number; and
h) Contact information of licensee (phone number or website).

4.2.02 Raffle Ticket Validation Numbers

The algorithm or method used by the Venue-Based ERS to generate ticket validation numbers must be unpredictable and ensure that duplicate validation numbers will not be re- generated for the raffle currently in progress.

4.2.03 Voiding a Raffle Ticket

If a raffle ticket is voided, the Venue-Based ERS must:

a) Record the draw number and validation number pertaining to the voided ticket for the raffle in progress or the raffle that has concluded;
b) Recognize the voided raffle ticket information, ensuring that a voided ticket will not affect the outcome of a valid raffle win; and
c) Record an acknowledgement from authorized licensee personnel that voided tickets have been reconciled before permitting a winning number to be entered into the system.

4.2.04 Sample or "Test" Raffle Tickets

If the RSU has the functionality to test the quality, performance, or reliability of a ticket by producing a sample or "test" ticket, then the ticket must have an obvious marking prominently displayed upon the ticket face so as to be easily discernable from a valid ticket. The ticket shall clearly indicate that there is no value associated with the test ticket.

4.2.05 Counterfoil Requirements

If an electronic RNG is not used to determine the winner(s) of a raffle, a counterfoil ticket must be used. A counterfoil ticket shall be printed or stored electronically for each draw number purchased for the raffle. The counterfoil ticket must identify the draw number that has been issued to the purchaser. In addition to the draw number, the following information must be available either printed on the counterfoil ticket, or stored electronically within the system:

a) Event identifier or location;
b) Additional contact information collected at the time of sale;
c) Date and time the ticket was issued in twenty-four (24) hour format showing hours and minutes;
d) Cost of the raffle ticket; and
e) Unique validation or barcode number.

4.2.06 Counterfoil Printer Error Conditions

If printed counterfoil tickets are required, the printer(s) used must be able to indicate the following error conditions:

a) Out of paper;
b) Memory error;
c) Printer jam/failure; and
d) Printer disconnected.

4.3.00 Raffle Prize Display

4.3.01 General

For Venue-Based ERS that support a monetary prize display intended to be viewed by participants of the raffle, the display shall indicate the raffle prize in Canadian funds using a calculation deemed acceptable by SLGA, and that shows progression of the prize amount, if applicable.

Note: It is accepted that communication delays can exist, dependent on vendor product and configuration, and the displayed prize amount may temporarily be different from the amount recognized in the system.

4.3.02 Winning Raffle Ticket Display

Once the winning draw number for the raffle has been determined, all raffle prize displays shall display the winning number in the location of the raffle for all participants to view.

4.4.00 Raffle Drawing Requirements

4.4.01 Closing the Raffle Purchase Period

The licensee will determine the closing time for the sale of raffle tickets for a given raffle and the Venue-Based ERS used must be capable of ceasing raffle ticket sales at this pre- determined time.

A raffle draw shall be conducted only after:

a) The close of the raffle; and
b) All sold and voided tickets have been reconciled for the particular raffle purchase period.

4.4.02 Winner Determination

The licensee shall conduct a manual draw or initiate an electronic draw procedure which ensures a randomly selected draw number is chosen from all tickets sold for that raffle. Voided tickets must not impact the outcome of the raffle draw.

4.4.03 Winning Ticket Verification

The Venue-Based ERS must be capable of verifying the winning draw number either manually or through the use of a barcode scanning device capable of reading the code on the raffle ticket.

4.5.00 Venue-Based Accounting Reports

4.5.01 Reports

The Venue-Based ERS must be capable of producing exportable general accounting and exception reports, which will include:

a) Information required for each raffle conducted:
    i. Date and time of event;
    ii. Licensee running the event;
    iii. Sales information including total sales, refunds, voids, etc.;
    iv. Prize distribution (total raffle sales vs. prize awarded to participant);
    v. Number of draw numbers in play; and
    vi. Winning number(s) drawn.
b) Exception Report identifying changes to the Venue-Based ERS including:
    i. System parameters;
    ii. Corrections;
    iii. Overrides; and
    iv. Voids.
c) The system must be able to generate a report that contains information collected by the RSU attendant at time of sale.
d) Sales-by-RSU Report that includes the following:
    i. Breakdown of individual RSU total sales;
    ii. Record of each RSU operator;
    iii. Breakdown of draw numbers sold using each RSU; and
    iv. Any voided and misprinted tickets.
e) Voided Draw Number Report that includes a list of all draw numbers that have been voided including validation numbers.
f) RSU Event Log that lists events recorded for each RSU. This includes:
    i. Date and time; and
    ii. Brief description of event (codes may be used for event identification).
g) RSU Corruption Log that lists all RSUs unable to reconcile to the system. This includes RSU identifier, RSU operator and money collected.

4.6.00 RSU Requirements

4.6.01 Attendant-Operated RSU

An RSU relies on hardware and software configurations to provide a purchaser with a raffle ticket when a fee is paid. The two (2) types of RSUs commonly used with a Venue-Based ERS are known as an attendant-operated RSU and a player-operated RSU. **Only Attendant-Operated RSUs are allowed in Saskatchewan.** An attendant-operated RSU requires a purchaser to pay a raffle ticket fee to an attendant. Upon receiving the payment the attendant will, using the RSU, print a ticket for the raffle which will be presented to the purchaser.

4.6.02 Access Controls

Access to raffle sales software shall be controlled by a secure logon procedure. The software must have the ability to lock up or logoff after a configurable amount of inactivity.

4.6.03 Touch Screens

Touch screens associated with the RSUs shall be accurate and if calibration is required, touch screen accuracy shall remain for the manufacturer's recommended maintenance period following the re-calibration.

4.6.04 Communications

RSU configuration will allow for the connection to and interaction with the Venue-Based ERS. An RSU must be designed or programmed such that it will only communicate with authorized Venue-Based ERS components.

4.6.05 Wireless Raffle Sales Units

Communication or data transfer must occur between the RSU and the Venue-Based ERS only through authorized access points.

4.6.06 Attendant Input

For raffles running longer than one day, the RSU shall have the capability to accept attendant input of information. The ability to enable or disable this functionality shall be managed in a controlled and auditable manner. **The RSU shall have, at minimum, the capability to acquire a ten-digit phone number of the purchaser.**

4.6.07 Critical Memory

Critical memory is used to store all data that is considered necessary to the operation of the RSU. Critical memory shall be maintained for the purpose of storing and preserving this data. This includes, but is not limited to:

a) Recall of all tickets sold including, at a minimum, draw numbers and validation numbers when not communicating with the system; and
b) RSU configuration data.

Note: Critical memory may be maintained by any component of the Venue-Based ERS.

4.6.08 Maintenance of Critical Memory

Critical memory storage must be maintained by a logical process that enables errors to be

identified. This process may involve signatures, checksums, partial checksums, multiple copies, time stamps and/or use of validity codes.

4.6.09 Comprehensive Checks
Comprehensive checks of critical memory shall be made on start-up and shall detect failures with a high level of accuracy.

4.6.10 Unrecoverable Critical Memory
An unrecoverable corruption of critical memory shall result in an error, which upon detection will cause the RSU to become inoperable.

4.6.11 Backup Requirements
Should a failure occur, the RSU must have a backup or archive feature or device which allows for the recovery of critical data.

4.6.12 RSU Program Requirements
All software programs shall contain sufficient information to be identified including the revision level of the information stored on the RSU. This may be displayed via a display screen. The software programs shall not be adversely affected by simultaneous activations of various inputs or outputs which might, whether intentionally or not, cause malfunctions.

4.6.13 Detection of Corruption
RSU software programs shall be capable of detecting program corruption and cause the RSU to cease operation until corrected.

4.6.14 Verification of Updates
Software updates must be successfully authenticated on the RSU prior to execution of the software update.

4.6.15 RSU Validation
The Venue-Based ERS must have the ability to identify and validate those RSUs that are in use for a raffle. This process confirms those RSUs issued and recognized by the system for the raffle.

4.7.00 Venue-Based ERS Servers
4.7.01 General
The following requirements are to be examined for Venue-Based ERS in addition to the requirements found in Part I

4.7.02 Security
The Venue-Based ERS Server(s) must be located within the facility. If the server(s) are intended to be housed outside the boundaries of the raffle, remote location of the server(s) will require SLGA approval. Access to the server(s) must be limited to authorized personnel.

4.7.03 Server Programming
The Venue-Based ERS must not allow the user to conduct programming on the server that may

result in modifications to the database. It is acceptable for Network Administrators to perform authorized network infrastructure maintenance or troubleshooting.

4.7.04 Synchronization Feature

If multiple clocks are supported, the system shall have a facility to synchronize clocks within all system components.

4.7.05 RSU Management

A Venue-Based ERS must have a master list of each authorized RSU in operation with the following information being included at a minimum for each entry:

a) A unique RSU identification number or corresponding hardware identifier (i.e. MAC address);
b) Operator identification; and
c) Tickets issued for sale, if applicable.

4.7.06 RSU Validation

It is recommended that each RSU be validated at pre-defined time intervals with at least one method of authentication. This time interval shall be configurable based on SLGA review and requirements. The system shall have the ability to remotely disable the RSU after the threshold of unsuccessful validation attempts has been reached.

4.7.07 Significant Events

Significant events must be communicated and logged on the Venue-Based ERS server(s) and may include:

a) Connection/disconnection of an RSU or any component of the system;
b) Critical memory corruption of any component of the system;
c) Counterfoil printer errors:
    i. Paper low;
    ii. No paper;
    iii. Printer failure;
    iv. Printer disconnect; and
    v. Memory error(s);
d) Establishment and failure of communications between sensitive Venue-Based ERS components;
e) Significant event buffer full;
f) Program error or authentication mismatch;
g) Firewall audit log full (if supported); and
h) Any other significant events or any event specified by SLGA.

4.7.08 Surveillance or Security Functionality

A Venue-Based ERS shall provide a facility that enables online searching of significant events through recorded data based on one or more of the following criteria:

a) Date and time range;
b) Unique component identification number; and
c) Significant event identifier.

4.8.00 Venue-Based Sales Communication Requirements

4.8.01 Communication Types

The Venue-Based ERS may use various methods of communication that may include, but are not limited to:

a) Ethernet connections;
b) Wireless communications protocol;
c) Bluetooth;
d) Cellular; and
e) Infrared.

The requirements that follow shall also apply if communications are performed across a public or third-party network as approved by SLGA.

4.8.02 Communication Protocol

Each component of a Venue-Based ERS must function as indicated by the communication protocol implemented and provide for the following:

a) Mutual authentication between any system component and the server(s);
b) All protocols used must offer communication techniques that have proper error detection and recovery mechanisms which are designed to prevent eavesdropping and tampering. Any alternative implementations will be reviewed on a case-by-case basis by SLGA;
c) Encryption methods shall be employed on all data communication critical to the raffle. The encryption algorithm shall employ variable keys or similar methodology to preserve secure communication.

4.8.03 Connectivity

Only authorized devices shall be permitted to establish connection/communication between any Venue-Based ERS components. The Venue-Based ERS shall provide a method to:

a) Verify that the system component is being operated by an authorized user;
b) Enroll and un-enroll system components;
c) Enable and disable specific system components;
d) Ensure that only enrolled and enabled system components participate in the raffle; and
e) Ensure that the default condition for components shall be un-enrolled and disabled.

4.8.04 Loss of Communication

If loss of communication occurs between an RSU and the Venue-Based ERS server(s) during the course of a raffle, the following is acceptable:

a) An RSU may continue to sell tickets when not in communication with the system and must synchronize at the earliest opportunity;
b) Raffle ticket sales taking place on the RSU during a loss of communication with the system shall be logged on the device;
c) If the RSU detects a buffer overflow limit during communication loss, the device(s) shall deactivate and remain in this state until the re-establishment of connection/communication to the system has occurred;
d) When the RSU has re-established connection/communication with the system, the RSU shall re-authenticate with the system server(s); and
e) Loss of communication shall not affect the integrity of the critical memory.

4.8.05 Wide Area Network (WAN) Communications

Generally, WAN communications are not allowed in Saskatchewan. A supplier may make a specific request for consideration on a case-by-case basis.

4.8.06 Wireless Local Area Network (WLAN) Communications

A WLAN provides connectivity to wireless devices within defined boundaries. Components of the WLAN that allow for communication are the host server and access points that serve as bridges between wired and wireless configurations. At a minimum, the following communication control applications should be used with a WLAN:

a) SSIDs should be hidden to prevent any attacks on the system;
b) WPA2 or higher encryption protocols;
c) MAC address filtering;
d) Segregation of network traffic; and
e) Other alternative wireless implementations which will be reviewed on a case-by-case basis by SLGA.

Part V
5.0.00 Online Prize Payments

5.1.00 Management

5.1.01 Prize Limits

SLGA reserves the right to restrict the total prize value of any raffle. The ERS shall have the capability to configure prize payout amounts.

5.1.02 Payments

Ticket purchasers have the option to have winnings paid directly through a payment gateway that is regulated by Canadian banking and credit card industries, e.g. PCI Data Security Standard. Payments will be allowed only if a way of ensuring financial accountability is possible by the ERS as follows:

a) A transaction can produce a sufficient audit trail and must not be processed until such time as the funds are received from the issuer or the issuer provides an authorization number indicating that the purchase has been authorized;
b) There must be a clear notification that the payment has been processed by the system and the details of the payment must be provided to the recipient once the payment is accepted;
c) Payment confirmation must include the amount processed by the ERS.

Definitions

Address Resolution Protocol (ARP) is the protocol used to translate IP addresses into MAC addresses to support communication on a wireless or wired local area network. The Address Resolution Protocol is a request and reply protocol and it is communicated within the boundaries of a single network, never routed across Internetwork nodes (connection points, either a redistribution point or an end point for data transmissions).

Algorithm is a finite set of unambiguous instructions performed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired result. Algorithms are the basis for most computer programming.

Authentication is a security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message or originator.

Bi-Directional is the ability to move, transfer or transmit in both directions

Bluetooth is a standard for the short-range wireless interconnection of cellular phones, computers and other electronic devices.

Buffer Overflow is the condition where the data transferred to a buffer (a temporary storage area) exceeds the storage capacity of the buffer and some of the data overflows into another buffer which could result in corruption of data.

Counterfoil is an electronic record or paper ticket stub, also known as a barrel ticket, which will be drawn to determine a winner and contains a player's draw number matching the basic ticket purchased and may, depending on the type of raffle, contain the name, address and/or telephone number of the player.

Crypto-analytic is an attack against the encryption key (refer to definition of encryption key).

Cryptographic is anything written in a secret code, cipher, or the like.

Distributed Denial of Service (DDoS) is a type of DoS attack where multiple compromised systems, usually infected with a destructive software program, are used to target a single system. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

Domain Used to identify one or more IP addresses. A domain name is used in a URL (Uniform Resource Locator) to identify particular Web pages.

Draw Numbers are defined as a number that is provided to the purchaser which may be selected as the winning number of the raffle.

Electronic Raffle System (ERS) is defined as any website, computer software, and/or related equipment used by raffle licensees for any or all of the following: sell tickets, account for sales, facilitate the selection of winners (and associated tasks); pay prizes.

Encryption is the reversible transformation of data from the original (the plaintext) to a difficult-to-interpret format (the cipher text) as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity.

Encryption Key is a sequence of numbers used to encrypt or decrypt (to decode/decipher) data.

Ethernet is defined as a system of connecting a number of computer systems to form a network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.

Firewall is any 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.

Geolocation refers to identifying the real-world geographic location of an Internet connected computer, mobile device, or website visitor.

Host refers to a computer system that is accessed by a user working at a remote location. Typically, the term is used when there are two computer systems connected by modems and telephone lines. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal.

Infrared is a wireless mobile technology for device communication over short ranges. Infrared communication requires line-of-sight configurations, has a short transmission range and is unable to penetrate walls.

Internet is an interconnected system of networks that connects computers around the world via Transmission Control Protocol/Internet Protocol, the suite of communications protocols used to connect hosts on the Internet.

Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Used in computer security, intrusion detection refers to the process of monitoring computer and network activities and analyzing those events to look for signs of intrusion in your system.

IP Address is short for Internet Protocol address and is an identifier for a computer or device on a TCP/IP network.

Licensee is an entity such as a person, business or organization that holds an approved license to conduct an activity.

Man-in-the-Middle (MITM) is an active Internet attack where the person attacking attempts to intercept, read or alter information moving between two computers.

Message Authentication is a security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.

Online refers to being connected to the Internet.

Protocol (Communication) is a set of formal rules describing how to transmit or exchange data, especially across a network. TCP/IP is the standard communications protocol of the Internet and most internal networks.

Raffle a form of lottery in which a number of persons buy one or more chances to win a prize.

Raffle Sales Unit (RSU) is defined as a portable or wireless device, a remote hard-wired connected device or a stand-alone cashier station that is used as a point of sale for raffle tickets.

Random Number Generator (RNG) is defined as a computational or physical device designed to generate a sequence of numbers or symbols that lack any pattern.

SHA-2 (Secure Hash Algorithm) is a cryptographic hash function (an algorithm that maps data of variable length to data of a fixed length) designed by the United States National Security Agency and is used for the protection of sensitive unclassified information. The SHA-2 algorithm takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value.

Shellcode
In hacking, a shellcode is a small piece of code used as a payload in the exploitation of a software vulnerability.

Security Certificate is information, often stored as a text file that is used by the TSL (Transport Socket Layers) Protocol to establish a secure connection. A Security Certificate contains information about whom it belongs to, who it was issued by, valid dates, a unique serial number or other unique identification that can be used to verify the contents of the certificate. In order for an TSL connection to be created, both sides must have a valid Security Certificate, which is also called a Digital ID.

SSID (Service Set Identifier) is a type of WLAN. All wireless devices on a WLAN must employ the same SSID in order to communicate with each other.

Validation Numbers are defined as a unique number which may represent one or more draw numbers that will be used to validate the winning number for the raffle.

WPA2 (Wireless Protected Access 2) is a security technology commonly used on Wi-Fi wireless networks. WPA2 is based on the IEEE 802.11i technology standard for data encryption.