Gaming Policy and Enforcement Branch (GPEB)

TGS6

Technical Gaming Standards for Electronic Raffle Systems

Technical Standards Document (TSD) Version 3.0

Gaming Policy and Enforcement Branch

3rd Floor, 910 Government Street
P.O. Box 9202 Stn. Prov. Govt.
Victoria, British Columbia, Canada
V8W 9J1

Revision Date: November 14, 2018

Table of Contents

1 Overview of TSD

1.1 Introduction

1.1.1 General Statements I

The General Statements are as follows:

a) Before being permitted to operate in the live environment, all gaming supplies used in the Province of British Columbia must be tested to the applicable requirements set forth in this Technical Standards Document (TSD).
b) For the purposes of this TSD, Electronic Raffle Systems are gaming supplies as defined in Section 1 of the *Gaming Control Act* of British Columbia.
c) A gaming service provider may select an Accredited Testing Facility (ATF), or other equivalent body, that has been accredited by and registered with the Gaming Policy and Enforcement Branch (GPEB), to perform the testing required in this document.
d) The appointed testing body must provide their final evaluation results, reports, and any additional documentation as may be required directly to GPEB for review, and where required, subsequent discussion.
e) GPEB may accept internal quality assurance testing on an Electronic Raffle System; however, reliance on the test results for the purposes of certification is at the discretion of GPEB.
f) In cases where an ATF does not perform tests that are required by or recommended in this document, GPEB may accept results from reputable testing companies. Reliance on these test results for the purposes of certification is at the discretion of GPEB.
g) Any ATF or other equivalent body that is employed to perform testing, and is approved by GPEB, must treat the gaming service provider as its client, and GPEB as the regulatory authority for issuing approvals. Although the appointed testing body may recommend the approval of any gaming supplies for use in the Province of British Columbia, the ultimate authority to approve gaming supplies rests solely with GPEB. Under Section 40 of the *Gaming Control Act* of British Columbia, only GPEB can issue rules about the use of gaming supplies during licensed gaming events. Only GPEB can issue a Certificate of Technical Integrity under the *Gaming Control Act* of British Columbia.
h) Each ERS must comply with applicable privacy legislation (e.g. PIPA). ATFs need not conduct any compliance testing related to privacy legislation; however, the ATF will report any obvious issues to GPEB and the gaming service provider for resolution.

1.1.2 General Statement II

This document will be updated when necessary to reflect changes in technology, testing methods, or cheating methods.

Note: *GPEB reserves the right to modify (or selectively apply) the requirements set forth in this TSD as deemed necessary to ensure the integrity of gaming in the Province of British Columbia. However, in order to ensure consistency and compliance, GPEB will not modify or selectively apply the requirements set forth in this TSD without first providing reasonable prior written notice to any gaming service provider, on an as-needed and case-by-case basis.*

1.2 Acknowledgment of Other TSDs Reviewed

1.2.1 General Statement

This TSD has been developed by reviewing and using portions of the documents listed below:

a) GLI (Gaming Laboratories International) Standard GLI-31 – Standards for Electronic Raffle Systems, Version 1.0 (November 16, 2012), and,
b) Liquor and Gaming Authority of Manitoba (LGA) Technical Standards for Electronic Raffle Systems.

1.3 Purpose of TSD

1.3.1 Purpose

The Purpose of this TSD is as follows:

a) To eliminate subjective criteria in analyzing and certifying Electronic Raffle Systems operation.
b) To only test those criteria which impact the credibility and integrity of Electronic Raffle Systems operation.
c) To create a TSD that will help ensure that Electronic Raffle Systems are fair, honest, secure, safe, auditable, and able to operate correctly.
d) To recognize that testing which does not impact the credibility and integrity of the Electronic Raffle System (such as Electrical Testing) should not be incorporated into this TSD, but left to appropriate test laboratories that specialize in that type of testing.
e) To recognize that except where specifically identified in this TSD, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer of the equipment.
f) To construct a TSD that can be easily changed or modified to allow for new technology or functionality.
g) To construct a TSD that does not specify any particular method or technology for any element or component of an Electronic Raffle System. The intent is instead to allow a wide range of methods and technologies to be used to comply with this TSD, while at the same time, to encourage new methods and technologies to be developed.

1.3.2 No Limitation of Technology

One should be cautioned that this TSD should not be read in such a way that limits the use of future technology. The TSD should not be interpreted that if the technology is not mentioned, then it is not allowed. As new technologies are developed, GPEB will review this TSD, make any changes deemed necessary, and incorporate new minimum standards for the new technology.

1.4 Other Documents That May Apply

1.4.1 Other TSDs

This TSD, as well as the other TSDs listed below, are to be interpreted so that all of the provisions are given as full effect as possible. In the event of a conflict or inconsistency between the foregoing, unless expressly stated to the contrary, the order of precedence shall be as follows:

a) This TSD (i.e. TGS6 – Electronic Raffle Systems),
b) TGS1 – Technical Gaming Standards for Electronic Gaming Devices (EGDs) in Gaming Venues, and,
c) TGS3 – Technical Gaming Standards for On-line Monitoring and Control Systems (MCSs) and Validation Systems in Gaming Venues.

1.4.2 GPEB Standards

This TSD must not contradict any provisions of the following standards:

a) Advertising and Marketing Standards for the BC Gambling Industry,
b) GPEB Responsible Gambling Standards, and,
c) GPEB's guidelines, conditions, and rules related to gambling event licences.

1.4.3 Legislated Acts or Regulations

This TSD must not contradict any provisions of the following legislation:

a) The *Criminal Code of Canada*,
b) The *Gaming Control Act* and *Gaming Control Regulation* of British Columbia, and,
c) The *Personal Information Protection Act (PIPA)* of British Columbia.

1.4.4 Information Systems Security (ISS) Industry Standards

The Administrative Controls, Technical Controls and Physical & Environment Controls for Electronic Raffle Systems should incorporate the best practice principles found in the applicable and relevant ISS industry standards, as dictated by such sources as:

a) ISO / IEC 27001 – Information Security Management Systems (ISMS),
b) ISO / IEC 27002 – Code of practice for information security management,
c) ISO 31000:2009 – Risk Management – Principles and guidelines,
d) Control Objectives for Information and Related Technology (COBIT), and,
e) Open Source Security Testing Methodology Manual (OSSTMM).

Before an ERS is approved, the gaming service provider may be required to provide evidence to GPEB about how the ERS and its related systems incorporate the principles described in sources such as those listed above.

1.5 Definitions

a) ATF (Accredited Testing Facility) – An accredited test facility/laboratory approved by GPEB for the purposes of gaming supply testing.
b) Counterfoil – An electronic record or a paper ticket stub, also known as a barrel ticket, which will be selected randomly to determine a winner and contains a single draw number matching the purchaser's ticket and may, depending on the type of raffle, contain the contact information for the purchaser that is required by the conditions of the licence.
c) Draw Number – A uniquely identifiable number that is provided to the purchaser for each chance to win that has been purchased. Each draw number is recorded in an electronic or paper counterfoil and is eligible to be drawn as the winning number for the raffle.
d) Electronic Raffle System (ERS) – Computer software and related equipment used by raffle licensees to sell tickets, account for sales, facilitate the manual or electronic drawing of tickets to determine the winners, and/or disburse prizes.
e) GPEB – Gaming Policy and Enforcement Branch.
f) Ticket – An electronic record or a paper ticket provided as a transaction receipt that is delivered to a purchaser and contains one or more draw numbers. Tickets must contain the information required by the conditions of the licence.
g) RNG – Random Number Generator.
h) RSU – Raffle Sales Unit. An RSU is comprised of a combination of hardware and software configured to operate as a point of sale that will generate and deliver raffle tickets to purchasers.
i) Validation Number – A unique number which may represent one or more draw numbers that will be used to validate the winning number for the raffle. A validation number may be encoded using automatic scanning technology (for example, a bar code or QR code scanning device) or be in human readable form.

1.6 Testing & Documentation

1.6.1 General Statement

An ERS may be certified and approved by GPEB for use in British Columbia if:
a) An approved ATF has tested the integrity of the system in a laboratory setting with the equipment assembled, and has confirmed that the ERS meets the standards outlined in this TGS.
b) The gaming service provider has provided a demonstration of the ERS, and any documentation required to assess the system, to GPEB.
c) As required by GPEB, on-site or remote testing performed by GPEB following each new installation of the ERS confirms that the system has been properly configured and that it can be operated effectively. This may include, but is not limited to, conducting event simulations with and without challenges to system operations, testing the stability of the system at maximum

anticipated loads, verifying the internal controls and IT infrastructure at the venue, and any other tests as mandated by GPEB.

d) As required by GPEB, security audit and/or penetration testing performed by a reputable testing company has confirmed that the ERS meets industry standard security requirements, and any security standards outlined in this document that have not been tested by an ATF.

1.6.2 Documentation

At the request of GPEB, gaming service providers must submit the following documents related to an ERS:

a) Operation and training manuals associated with the ERS,
b) Technical Service manuals which:
    i. Accurately depict the system which the manual is intended to cover,
    ii. Provide adequate detail and are sufficiently clear in their wording and diagrams to support interpretation by GPEB 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 enable appropriate staff to make a record of the work performed and the results of the inspection,
    v. Include a complete list and samples of available reports that can be generated by the system,
c) Technical documentation that must provide adequate detail and be sufficiently clear in wording and diagrams to enable the review/evaluation of the system used, and,
d) Complete documentation for programming patches, fixes and any upgrades made to the system.

2 Electronic Raffle Systems (ERS) Management

2.1 General Operating Procedures

2.1.1 General Statement

An Electronic Raffle System (ERS) will have one or more of the following:

a) An electronic method for selling and/or distributing tickets (for example, through hardware based Raffle Sales Units [RSUs] or an online interface). An ERS may also be used to facilitate ticket sales and ticket distribution through other channels, such as over the telephone or in-person, and in such cases, must have systems designed to conduct these sales with sound inventory control and management.
b) The tools necessary for the collection, tracking, and accounting of all transactions initiated through the raffle system.
c) The ability to support all RSUs, whether they are hard-wired or connected wirelessly, to ensure that each unit sends or transmits all ticket sales to the system.
d) A solution that facilitates the printing and collection of paper counterfoils for use in a manual draw process that ensures that each counterfoil has an equally likely chance to be drawn.
e) A solution that facilitates the generation of a random winning selection by electronic means from all counterfoils and ensures that each counterfoil has an equally likely chance to be drawn.
f) A mechanism that provides for distribution of prizes online, which can verify that the prize is delivered to the correct prize winner.

2.1.2 Licence Compliance

An ERS must be capable of operating in a manner that fully complies with the licence conditions and rules of play under which the licence has been issued.

2.1.3 Prize and Sales Limitations

If required by the licence conditions, an ERS must be capable of configuring limits for:

a) The maximum prize that may be won,
b) The maximum number of tickets that may be sold, and,
c) The price for which tickets may be sold.

2.1.4 System Configuration Changes

The ERS must ensure that configuration settings cannot be modified without an authorized secure logon. Once a raffle has commenced, system configuration changes shall not be allowed until the completion of the raffle. Any configuration changes must be logged by the system.

2.1.5 Terms and Conditions

The ERS must employ a procedure to ensure that ticket purchasers:

a) Are eligible to participate in the raffle, and,
b) Have agreed to all of the necessary privacy policies, terms, and conditions of participating in the raffle. This may be accomplished by:
    i. Having ticket purchasers register for a secure purchaser account on an online system,
    ii. Requiring that ticket purchasers acknowledge the privacy policy and terms and conditions on a raffle sales unit (RSU),
    iii. Referring to the eligibility criteria, privacy policies, terms, and conditions on printed tickets, and stating that purchase of the ticket implies agreement with these requirements, or,
    iv. Another procedure approved by GPEB.

2.1.6 Purchase Location

If required by the licence conditions, an ERS that offers online ticket sales must have in place a

mechanism to ensure that ticket purchasers are located in the British Columbia. This must be accomplished by notification on the sales interface that only individuals currently located in the province may purchase a ticket and a check box to be completed by the purchaser attesting to that fact that they are located in B.C. Additionally, geolocation software may be used to confirm the location of the ticket purchaser.

2.2 Tickets & Counterfoils

2.2.1 General Statement

a) An ERS must be capable of generating raffle tickets with one or more uniquely identifiable draw numbers.
b) For each draw number generated, there must be one and only one matching counterfoil with the same draw number. The system must generate a unique counterfoil for each draw number sold on a ticket. The system must not generate duplicate draw numbers within the same event.
c) When an ERS is being used to conduct a raffle, it must be able to only generate tickets and counterfoils for that raffle.
d) The ERS must not generate additional counterfoils for ticket reprints.
e) All counterfoils used in a raffle drawing must be entered into the system electronically or printed for each purchased draw number.
f) Printed counterfoils must be the same size, shape, and weight.
g) All counterfoils must have an equal chance of being selected.

2.2.2 Required & Optional Information – Tickets & Counterfoils

a) A purchaser shall receive a ticket as a transaction record for one or more chances to win in a raffle draw. The ticket may be generated physically or electronically.
b) Each ticket and counterfoil must be configurable to physically or electronically record the information required by the licence conditions.
c) Each ticket and counterfoil must include the time and date that it was issued.
d) A ticket may contain additional printed information (e.g. advertising, logos, coupons, etc.). Some of this information may be contained on the ticket stock itself. Any additional printed information must not impact or obscure the information required to appear on the ticket.

2.2.3 Validation Numbers

Each ticket must be issued with a unique validation number, in human readable form or encoded using automatic scanning technology (for example, a bar code or QR code scanning device). The algorithm or method used by the ERS to generate the validation number must be unpredictable and must ensure that there is no duplication of validation numbers for the raffle currently in progress.

2.2.4 Voiding a Ticket

The ERS must be capable of voiding a ticket after a sale has been completed.
a) Tickets must be voided within the ERS platform application by the system administrator or authorized personnel. It must not be possible to void a ticket from an RSU.
b) If a ticket is voided, the appropriate information, which includes the draw number(s) and the validation number(s) pertaining to the voided ticket, shall be recorded in the ERS.
c) Voided draw numbers shall not be available for re-sale or re-issue.
d) The ERS must flag or otherwise identify in the system, a voided ticket and its corresponding draw number(s) in support of the winning number validation process.
e) The ERS must require an acknowledgement by the system administrator or authorized personnel that voided tickets have been reconciled before permitting a winning number to be entered into the system.
f) The ERS must automatically adjust the total sales figure when a ticket is voided.

2.3 Raffle Prize Display

2.3.1 Active Prize Display

An ERS may support a display of either the current prize or the current gross sales that is intended to be viewed by purchasers of raffle tickets. The prize or gross sales shall be displayed in Canadian Dollars in a way that represents the current progression of the prize. If the gross sales are represented on the display, the display must include a message indicating the value of the prize.

***Note**: It is accepted that, depending on the medium and system configuration, communication delays may prevent an accurate reconciliation between the displayed prize jackpot and the system prize jackpot at any given point during the conduct of the event.*

2.3.2 Winning Draw Number Display

When an ERS displays the winning draw number of a raffle:
a) The display shall indicate the winning draw number in the same format as the ticket, and,
b) It shall display the winning number on all capable display devices that are intended to be viewed by purchasers.

2.4 Closing Sales

2.4.1 General Statement

The ERS must have the ability to limit the time period during which tickets may be purchased and limit the number of tickets available for sale. Upon expiration of the purchase period and/or completion of sale of the final ticket, the ERS must be capable of closing sales automatically.

2.4.2 Time of Closing

The time of the sales closing may be:
a) Configurable within the ERS, and,
b) Manually enabled by the licensee.

2.4.3 Sales Closure

a) Upon closure of sales, the ERS must display to the system administrator that all sales from RSU devices and/or the on-line platform have been uploaded, transferred or otherwise communicated to the server.
b) On verification of the sales data transfer, all RSUs and online interfaces must be closed and rendered incapable of ticket sales for the closed raffle.

2.4.4 Time and Ticket Counter Display

The ERS must be capable of displaying by way of the RSUs and/or on-line the time and/or the number of tickets remaining until sales are closed. The sales closure, when it occurs, must also be displayed.

2.4.5 Reconciliation

The ERS must be capable of reconciling all sales, including sold, unsold and voided sales for the raffle purchase period to ensure that only valid draw numbers are eligible to win.

2.5 Winner Determination

2.5.1 General Statement

The ERS will be capable of allowing the licensee to randomly select a winning draw number or draw numbers from all valid draw numbers issued during the period of the raffle, in a way that complies with all of the rules and conditions of their license.

2.5.2 Manually Drawn Counterfoil Validation

On completion of a manual draw, the ERS must have the facility to verify the status of the drawn counterfoil number (i.e. valid draw number or voided draw number).

2.5.3 Winner Verification

a) The ERS must be capable of verifying the winning ticket presented by the purchaser to the licensee either manually, or if applicable, through the use of automatic scanning technology (for example, a bar code or QR code scanning device) reading the validation number.
b) After verification, the ERS must record and retain the winning number within the system database.

2.6 Accounting Reports

2.6.1 General Statement

The ERS must be capable of producing exportable general accounting reports and exception reports.

2.6.2 Standard Event Reporting

The following data will be maintained for each raffle drawing:
a) Date and time of event,
b) Licensee identification,
c) Sales information (sales totals, refunds, voids, reprints, and sales by price point),
d) Prize distribution (including prize award to winning participant and revenue retained by licensee),
e) Refund totals by event,
f) Draw numbers-in-play count,
g) Winning number(s) drawn (including draw order, call time, and claim status), and,
h) Other reports as required by GPEB.

2.6.3 Accounting Reports

The ERS must be capable of producing and exporting the reports listed in this section, if the reports are applicable to the system's functionality. All activities on the following reports must be date and time stamped, and the reports sortable by any field.
a) Error/Exception Report – Exception information including, but not limited to, changes to the raffle configuration, corrections, overrides, reprints of tickets and counterfoils, and voids.
b) Ticket Report – A report which includes a list of all tickets sold including all associated draw numbers and selling price points.
c) Sales by RSU – A report which includes a breakdown of each RSU's total sales, including draw numbers dispensed and any voided or misprinted tickets or reprint requests.
d) Sales Summary by Price Point – A report that summarizes the number of tickets sold at a particular price point and expresses the total dollar value of the sales for each. The summary should also provide an aggregate total for this information.
e) Voided Draw Number Report – A report which includes a list of all draw numbers that have been voided, including corresponding validation numbers.

f) RSU Event Log – A report which lists all events recorded for each RSU, including the date & time, a brief text description of the event and/or identifying code.
g) RSU Corruption Log – A report which lists all RSUs that are unable to be reconciled to the system, including the RSU identifier, RSU operator, and the money collected.

3 Raffle Sales Unit (RSU) Requirements

3.1 Introduction

3.1.1 General Statement

a) An RSU is comprised of a combination of hardware and software configured to operate as a point of sale that will generate and print or deliver raffle tickets.
b) Tickets may be purchased either from an attendant-operated RSU, a player-operated RSU, or an Online Interface. Any other methods will be reviewed and approved by GPEB on a case-by-case basis.

3.2 RSU Types

3.2.1 Attendant-operated RSU

a) Tickets may be sold by an attendant. Upon receiving payment for the ticket, the attendant will cause the RSU to generate and print a ticket with the corresponding draw numbers based on the purchaser's request and the pricing model for the raffle.
b) It is permitted that the attendant-operated RSU may be configured as a mobile/wireless option or as a fixed connection option.

3.2.2 Player-Operated RSU

a) Tickets may be sold by a stand-alone sales unit that has been correctly configured for the current raffle. A participant can make a purchase following the instructions appearing on the screen of the player-operated RSU. Upon verification of payment, the RSU will print and dispense or cause to be delivered a ticket with the corresponding draw numbers to the purchaser based on the purchaser's request and the pricing model for the raffle.
b) A player-operated RSU must be configured with a fixed connection option.

3.2.3 Online Interface

a) Tickets may be sold through online interfaces that have been correctly configured for the current raffle. Upon verification of payment, the RSU will deliver a ticket with the corresponding draw numbers to the purchaser based on the purchaser's request and the pricing model for the raffle. Tickets may be delivered electronically or physically.
b) For testing purposes, online interfaces will be treated as another form of RSU. All of the standards in this document applicable to online sales will be applied to testing online interfaces used as RSUs.

3.3 Raffle Sales Unit Operations and Security

3.3.1 Access Controls

a) Access to raffle sales software on Raffle Sales Units (RSUs) shall be controlled by a secure logon procedure. The software must have the ability to automatically lock up or logoff after a system-configurable amount of inactivity. Reasonable thresholds for the length of inactivity before lock up or logoff will be implemented for each technology used.
b) An RSU must be configured with a unique identifier that is recorded in the ERS.
c) It must not be possible to modify the configuration settings of the RSU without an authorized secure logon.

3.3.2 Communications

a) An RSU must be designed or programmed such that it may only communicate with authorized ERS components. An RSU will use industry standard communication methodologies and

technologies as detailed in Chapter 5 – Communication and Connectivity Requirements of this standard.

b) An RSU may use any of the industry standard communication technologies noted in Chapter 5 of this TSD as a primary means of communication and/or data transfer provided that one or more other technologies are available as a backup in the event of primary communication failure.

c) Communications and/or data transfer must only occur between the RSU and the ERS system via authorized access points.

3.4 Critical Memory Requirements

3.4.1 Critical Memory Defined

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

a) When not communicating with the system, recall of all tickets sold including, at a minimum, draw numbers and validation numbers, and,

b) RSU configuration data.

Note: *Critical memory may be maintained by any component(s) of the ERS.*

3.4.2 Maintenance of Critical Memory

Critical memory storage shall be maintained by a methodology that enables errors to be identified. This methodology may involve signatures, checksums, partial checksums, multiple copies, time stamps and/or effective use of validity codes.

3.4.3 Comprehensive Checks

It is recommended that critical memory be continuously monitored for corruption. Failures of critical memory shall be detected with an extremely high level of accuracy.

3.4.4 Unrecoverable Critical Memory

An unrecoverable corruption of critical memory shall result in an error. Upon detection, the raffle sales unit shall cease to function.

3.4.5 Backup Requirements

The RSU must have a backup or archive utility, which allows for the recovery of critical data should a failure occur.

3.5 RSU Program Requirements

3.5.1 Identification

All programs shall contain sufficient information to identify the software version and revision level of the information stored on the RSU, which may be displayed via a display screen.

Note: *The process used in the identification of the software and revision level will be evaluated on a case-by-case basis.*

3.5.2 Detection of Corruption

RSU programs shall be capable of detecting program corruption on start-up and cause the RSU to cease operations until corrected.

***Note**: Program verification mechanisms will be evaluated on a case-by-case basis and approved by the ATF laboratory based on industry-standard security policies.*

3.5.3 Verification of Updates

Prior to execution of updated software, the software must be successfully authenticated on the RSU.

3.6 RSU Management Requirements

3.6.1 RSU Management Functionality

An ERS must have a master list of each authorized RSU in operation, including at a minimum, the following information for each RSU:

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

***Note**: If these parameters can be retrieved directly from the RSU, sufficient controls must be in place to ensure accuracy of the information.*

3.6.2 RSU Validation

It is recommended that RSUs be validated at pre-defined time intervals with at least one method of authentication. This time interval shall be configurable based on GPEB requirements, in consultation with the gaming service provider and/or the licensee during on-site or remote testing. The system shall have the ability to remotely disable the RSU after the threshold of unsuccessful validation attempts has been reached.

3.7 Independent Control Program Verification

3.7.1 General Statement

The RSU shall have the ability to allow for an independent integrity check of the RSU's software from an outside source. This is a requirement for all RSU software that may affect the integrity of the raffle. This may be accomplished by being authenticated by a third-party device, or by allowing for the removal of the media such that it can be verified externally. Other methods shall be evaluated on a case-by-case basis. This integrity check will provide a means of field verification of the software to identify and validate the program. The ATF, prior to device approval, shall evaluate the integrity check method.

***Note**: If the authentication program is within the RSU software, the manufacturer must receive written approval from the authentication program vendor prior to submission and testing by the ATF.*

3.8 RSU Raffle Ticket Printer

3.8.1 General Statement

The RSU ticket printer that is used to generate a paper ticket shall be configured to print the information as detailed in Section 2.2.2 of this standard.

***Note**: It may be permissible for some of this information to be contained on the ticket stock itself.*

3.8.2 RSU Printer Configuration

a) The RSU ticket printer must be connected to the RSU sales device using one of the industry

standard communication technologies described in Chapter 5 of this TSD as a primary communication method.

b) The RSU must control the transfer of ticket data sent to the RSU printer, and only transfer ticket data to the printer when sufficient space is available in the RSU printer memory to receive the ticket information.
c) If a barcode forms part of the validation number printed on the ticket, the printer must support the barcode format and print with sufficient resolution to permit validation by a barcode reader.
d) The printer must be capable of detecting a low paper/out of paper condition and must cease operation and alert the operator to the need to load new paper.
e) The printer must be capable of detecting a low battery condition and alerting the operator.
f) If the RSU ticket printer is capable of reprinting a ticket, the reprinted ticket shall clearly indicate that it is a reprint of the original ticket.

4 Electronic Raffle System (ERS) Platform

4.1 Introduction

4.1.1 General Statement

ERS platform servers must be located in a single facility, either at the event location or remotely within Canada. In all cases, the platform servers must be protected by appropriate physical and logical security.

4.1.2 Third Party Hosting

Where one or more components of the ERS are hosted by a third party service provider, the following requirements must be met:

a) The third party service provider must be a reputable company that is capable of meeting the information security standards described in this document.
b) Evidence that the third party service provider complies with the information security standards outlined in this document must be provided to GPEB prior to approval of the ERS, and may be required on an ongoing basis. This evidence may take the form of audits conducted by independent, accredited auditing bodies.
c) Copies of the agreement(s) with the third party service provider must be provided to GPEB for review and discussion to ensure that all relevant requirements are included.
d) All gambling transactions and related data processing/storage must take place in Canada.
e) Critical files will be monitored and verified by GPEB as described in section 4.8.1 of this document.

4.1.3 Asset Management

A designated system administrator must be responsible for ensuring that information and computer assets related to the ERS are appropriately classified, and defining and periodically reviewing access restrictions and classifications. This may be verified during on-site testing by GPEB.

4.2 General Operation and Server Security

4.2.1 Physical Security

The servers shall be housed in a secure location that has sufficient physical protection against alteration, tampering or unauthorized access. GPEB may require on-site testing or a security audit to verify the physical security of ERS servers.

4.2.2 Logical Security

a) The ERS must be logically secured by means using generally accepted practices for IT network security which may include but is not limited to one or more of the following technologies:
    i. Passwords,
    ii. PINs,
    iii. Authentication credentials (i.e. magnetic swipe, proximity cards, embedded chip cards), and,
    iv. Biometrics.
b) The ERS must have multiple security access levels to control and restrict different classes of access to the system.
c) The ERS must be configured for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts.

4.2.3 Access Controls

The allocation of access privileges shall be restricted and controlled according to business

requirements and the principle of least privilege.

a) A formal user registration and de-registration procedure must be in place for granting and revoking access to all information systems and services.
b) All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
c) The use of generic accounts shall be limited, and where used, the reasons for their use shall be formally documented.
d) Password provision must be controlled through a formal management process.
e) Passwords must meet business requirements for length, complexity and lifespan.
f) Access to system applications shall be controlled by a secure log-on procedure.
g) Appropriate authentication methods, in addition to passwords, shall be used to control access by remote users.
h) Any physical access to areas housing components used for the sale of ticket(s) through an Internet application and any logical access to these applications must be recorded.
i) The use of automated equipment identification to authenticate connections from specific locations and equipment shall be formally documented and must be included in the regular review of access by management.
j) Restrictions on connection times shall be used to provide additional security for high-risk applications.
k) The use of utility programs that might be capable of overriding system application controls shall be restricted and tightly controlled.
l) A formal policy shall be in place and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

4.2.4 Security from Alteration, Tampering, or Unauthorized Access

The ERS shall provide a logical means of securing the system data against alteration, tampering or unauthorized access. The following rules also apply to the raffle data within the ERS.

a) No equipment shall have a mechanism whereby an error will cause the system data to automatically clear.
b) Data shall be maintained at all times regardless of whether the server is being supplied with power.
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.

4.2.5 Data Alteration

The ERS must not permit the alteration of any accounting, reporting or significant event data without supervised access controls. In the event any data is changed, the following information shall 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 the alteration (through login credentials).

4.2.6 Server Programming

The ERS platform must be sufficiently locked down to prevent any user initiated programming capabilities on the server in relation to the ERS application. It is acceptable for a network administrator to perform authorized network infrastructure maintenance or application troubleshooting.

4.2.7 Virus Protection

The ERS must have adequate and up to date virus protection.

4.2.8 UPS Support

a) Where the platform is a stand-alone application, it must have an Uninterruptible Power Supply (UPS) connected and of sufficient capacity to permit a graceful shut-down and that retains all ERS data during a power loss.
b) It is acceptable that the ERS server may be a component of a network that is supported by a network-wide UPS provided that the ERS server is included as a device protected by the UPS.

4.3 System Clock Requirements

4.3.1 System Clock

An ERS must maintain an internal clock that reflects the current date and time (in twenty-four (24) hour format showing hours, minutes, and seconds) that shall be used to provide the following:
a) Time stamping of significant events,
b) Reference clock for reporting, and,
c) Time stamping of all sales and draw events.

4.3.2 Synchronization Feature

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

4.4 Platform (Counterfoil) Printers

4.4.1 General Statement

The configuration of printers used for the printing of counterfoils must have sufficient capacity to print the number of counterfoils based on the expected volume of ticket sales and within the time frame set for the conduct of the raffle.

4.4.2 Physical Printer Configuration

The design of the physical layout of the counterfoil printers must ensure that all printed counterfoils are available to be drawn using the manual draw process as specified in the licence rules. With the exception of paper or paper roll changes, the configuration must not rely on any operator intervention to ensure that every printed counterfoil is collected properly.

4.4.3 Printer Specifications

All printers used in the platform configuration must be capable of printing counterfoils in the format described in Section 2.2 of this standard.

4.4.4 Low Paper Condition

a) All printers must have the ability to detect a low paper condition and alert the operator.
b) On detection of a low paper condition:
    i. The printer must have the capacity to complete the current print request,
    ii. The printer must not accept any further print requests and will remain unavailable until the low paper condition has been resolved, and,
    iii. On resolution, the printer must become available to the system without requiring an operator to reconfigure the printer settings.
c) At no time should a printer be available to the system to print a counterfoil ticket without paper.

4.4.5 Printer Disable

At any time during an active draw, the operator must have the ability to manually disable a printer and remove the printer from the configuration without affecting the remaining printers or any outstanding print requests.

4.5 Significant Events

4.5.1 Event Logging

a) Significant events shall be communicated and logged on the ERS server. Significant events include, but are not limited to:
   i. Power reset or failure of any component of the system,
   ii. Critical memory corruption of any component of the system,
   iii. Counterfoil printer errors (including low paper, out of paper, printer disconnection/failure to print, or buffer full),
   iv. Establishment and failure of communication between sensitive ERS components,
   v. Significant event buffer full,
   vi. Program error or authentication mismatch,
   vii. Firewall audit log full, where supported,
   viii. Intrusion Detection System/Intrusion Prevention System audit log full, where applicable,
   ix. Remote access, where supported,
   x. RSU event log,
   xi. RSU corruption log, and,
   xii. Any other significant events as specified by GPEB.
b) An ERS shall provide an interrogation program that enables on-line comprehensive searching of the significant events log through recorded data. The interrogation program shall have the ability to perform a search using one or more on the following criteria:
   i. Date and time range,
   ii. Unique component identification number, and,
   iii. Significant event identifier.

4.6 Backups, Recovery and Shutdown

4.6.1 Storage Medium Backup

The ERS shall have sufficient 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 on the ERS with open support for backups and restoration.

a) 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.
b) 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.

4.6.2 Recovery Requirements

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

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

4.6.3 Shutdown Requirements

The ERS must have the following shutdown and recovery 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.
b) The ERS must be able to identify and handle the situation where master resets have occurred on system components.
c) The ERS must have the ability to recover all critical information from the last backup.
d) 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 should be recoverable.

4.7 Data Archiving

4.7.1 General Statement

The ERS must be capable of creating an archival data set for each draw conducted. This data set must contain at a minimum:

a) All of those aspects of standard event reporting as noted in Section 2.6.2 of this standard, and,
b) All of those aspects of accounting reporting as noted in Section 2.6.3.

4.8 Authentication of System Software

4.8.1 General Statement

a) System software components and modules shall be authenticated by a secure means at the system level denoting Program ID and version. The system shall have the ability to allow for an independent integrity check of the components and modules from an outside source. This is a requirement for all software that may affect the integrity of the system. This may be accomplished by being authenticated by a third-party device, or by allowing for the removal of the 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 the programs or files. The ATF, prior to system approval, shall approve the integrity check method.
b) GPEB may allow or require that the critical software described in this section be monitored for changes by file integrity monitoring (FIM) software. If FIM software is used to monitor an ERS, it must:
   i. Be set up to automatically notify GPEB of any changes that take place in the critical files, and,
   ii. Maintain a log of changes to the critical files.

***Note**: If the authentication and/or file integrity monitoring programs are contained within the ERS software, the manufacturer must receive written approval from the authentication program vendor prior to submission.*

4.8.2 Version History Report

The ERS must be capable of generating a report showing the current software revision, date installed, previous (historical) software versions, dates installed and removed. This report should also contain login ID and IP/MAC addresses denoting where the commands originated for the actions performed.

5 Communication and Connectivity Requirements

5.1 Introduction

5.1.1 General Statement

Subject to the standards outlined in this chapter, an ERS may use one or more industry standard communication methods, including wireless networks. The requirements of this chapter shall also apply if communications are performed across a public or third party network, as approved by GPEB.

5.1.2 Communication Protocol

Each component of an ERS must function as indicated by the communication protocol implemented. Communications shall be demonstrably secure against crypto-analytic attacks. The encryption key(s) used to provide security to the system that provides for the sale of tickets through the Internet must be monitored and maintained. An ERS system must provide the following:

a) Mutual authentication between any system component and the server where a communication technology is utilized,
b) Protocols 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 with GPEB approval,
c) Industry standard encryption for all communications critical to the raffle,
d) Personally identifiable information, sensitive account data and financial information must be protected over a public network,
e) The failure of any single item should not result in denial of service,
f) An Intrusion Detection System/Intrusion Prevention System must be installed on the network to protect against known and emerging threats. The system must keep a record of its activity in an audit log,
g) Stateless protocols (e.g. UDP) should not be used for sensitive data without stateful transport, and,
h) All changes to network infrastructure (e.g. network device configuration) must be logged.

***Note**: Although HTTP is technically stateless, if it runs on TCP which is stateful, this is allowed.*

5.1.3 Cryptographic Controls

Cryptographic controls must be implemented for the protection of information.

a) Any sensitive or personally identifiable information must 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 organization acceptable to GPEB.
d) The grade of encryption used must be appropriate to the sensitivity of the data.
e) The use of encryption algorithms must be reviewed periodically by qualified management or 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.
g) Encryption keys must not be stored without being encrypted through a different encryption method and/or by using a different encryption key.

5.1.4 Bi-Directional Requirements

Significant emphasis shall be placed on the integrity of the communication system for bi-directional 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 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 appropriately secure forms of protection via encryption, segregation of information, firewalls, passwords and personal identification numbers.

5.1.5 Connectivity

Only authorised devices shall be permitted to establish communications or connectivity between any system components. The 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.

5.1.6 Loss of Communications - RSU

a) It is permitted that RSUs may continue to sell tickets when not in communication with the ERS. Sales transactions taking place on the RSU during a loss of communication with the ERS shall be stored or cached on the RSU. The RSU shall disable sales upon detecting the limit of its buffer overflow or cache limits.
b) Reasonable buffer/cache limits must be established in order that upon re-establishment of communications, the ERS is able to accommodate the load.
c) Upon the re-establishment of communication, the system shall require that the RSU re-authenticates with the ERS and transmits, uploads or otherwise transfers all sales transactions completed during the communication loss.
d) Loss of communications shall not affect the integrity of critical memory.
e) In the event that the primary means of communication is not recoverable within the period of the raffle draw, the RSU must be capable of transmitting, uploading, or otherwise transferring the cached sales data to the ERS using a secondary means of communication.

5.2 System Security

5.2.1 General Statement

Where an ERS is configured for internet connectivity, all communications, including remote access, must pass through at least one approved firewall and must not have a facility that allows for an alternate network path. Any alternate network path existing for redundancy purposes must also pass through a least one firewall.

5.2.2 Firewall Audit Logs

The firewall application must maintain an audit log and must disable all communications and generate a significant event which meets the requirements as specified in Section 4.6 Significant Events of this standard if the audit log becomes full. 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, port number and MAC addresses.

***Note**: A configurable parameter "unsuccessful connection attempts" may be utilized to deny further connection requests should the re-defined threshold be exceeded. The system administrator must also be notified.*

5.3 Remote Access

5.3.1 General Statement

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 only be allowed if authorized by GPEB; otherwise it must be disabled.

5.3.2 Remote Access

a) Where and when permitted, remote access shall accept only the remote connections permissible by the firewall application and ERS settings.
b) The ERS must be configured to deny the following functionality to a remote user:
   i. User administration functionality (adding users, changing permissions, etc.),
   ii. Access to any database other than information retrieval using existing functions, and,
   iii. Access to the operating system.
c) Remote access security and permitted functions during a remote access session will be reviewed on a case-by-case basis, in conjunction with the implementation of the current technology and approved by GPEB.

***Note**: GPEB acknowledges that the system manufacturer may, as needed, remotely access the ERS and its associated components for the purpose of product and user support, as permitted.*

5.3.3 Remote Access During a Raffle

a) The ERS must be capable of disabling remote access during the period of an active raffle game.
b) Remote access during an active raffle game can only be authorized and granted by the local, on-site administrator through the issuance of a temporary password.

5.3.4 Remote Access Auditing

The ERS must maintain an activity log which updates automatically depicting all remote access information, to include:
a) Log on name,
b) Time and date the connection was made,
c) Duration of the connection, and
d) Activity while logged in, including the specific areas accessed and any changes that were made.

5.4 Wide Area Network Communications

5.4.1 General Statement

Wide Area Network (WAN) communications are permitted as approved by GPEB and shall meet the following requirements:
a) The communications over the WAN are secured from intrusion, interference and eavesdropping via techniques such as the use of a Virtual Private Network (VPN), encryption, etc.
b) Only functions documented in the communications protocol shall be used over the WAN. The protocol specification shall be provided to the ATF.

5.5 Wireless Network Communications

5.5.1 General Statement

Should a wireless communication solution be utilized, it is recommended to adhere to the applicable portions of the chapter pertaining to wireless networks in the GLI-27 Standard – Network Security Best Practices.

***Note**: Due to continuous changes and improvements in wireless technology, the information in this document is considered current as of the publication date. Therefore, it is imperative for the manufacturer to review and update internal control policies and procedures to ensure the ERS is secure and threats and vulnerabilities are addressed accordingly.*

6 Random Number Generator Requirements

6.1 Introduction

6.1.1 General Statement

The selection process for the winning number shall be random. This may be accomplished through the use of an approved random number generator. The regulations within this section are only applicable to electronic raffle systems in which a Random Number Generator is utilized.

6.2 Random Number Generator (RNG) Requirements

6.2.1 Game Selection Process

An RNG shall reside on a Program Storage Device secured in the logic board of the system. The numbers selected by the RNG for each drawing shall be stored in the system's memory and be capable of being output to produce a winning number.

a) **All Outcomes Shall be Available** – Each valid, sold raffle number shall be available for random selection at the initiation of each drawing.
b) **No Corruption from Associated Equipment** – An electronic raffle system shall use appropriate protocols to protect the random number generator and random selection process from influence by associated equipment, which may be communicating with the electronic raffle system.
c) **RNG Integrity Standard** – The RNG and random selection process shall be impervious to influences from outside the electronic raffle system, including, but not limited to, electromagnetic interference, electro-static interference, and radio frequency interference.

6.3 Electronic Random Number Generator Requirements

6.3.1 General Statement

The use of an RNG results in the selection of raffle outcomes in which the selection shall:

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

6.3.2 Applied Tests

The test laboratory may employ the use of various recognized tests to determine whether or not the random values produced by the random number generator pass the desired confidence level of 99%. These tests may include, but are not limited to:

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

n) Tests on subsequences, and,
o) Poisson distribution.

NOTE: *The ATF will choose the appropriate tests on a case by case basis depending on the RNG under review.*

6.3.3 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.

6.3.4 Range

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

6.3.5 Background RNG Cycling/Activity Requirement

In order to ensure that RNG outcomes cannot be predicted, adequate background cycling/activity must be implemented between each drawing at a speed that cannot be timed. The rate of background cycling/activity must be sufficiently random in and of itself to prevent prediction.

NOTE: *GPEB recognizes that some times during the raffle, the RNG may not be cycled when interrupts may be suspended. This is permitted although this exception shall be kept to a minimum.*

6.3.6 RNG Seeding/Re-Seeding

The methods of seeding or re-seeding implemented in the RNG must ensure that all seed values are determined securely, and that the resultant sequence of outcomes is not predictable.

a) The first seed shall be randomly determined by an uncontrolled event. After every ticket draw, there shall be a random change in the RNG process (new seed, random timer, delay, etc.). This will verify the RNG doesn't start at the same value, every time. It is permissible not to use a random seed; however, the manufacturer must ensure that the selection process will not synchronize.
b) Unless proven to have no adverse effect on the randomness of the RNG outcomes, or actually improve the randomness of the RNG outcomes, seeding and re-seeding must be kept to an absolute minimum. If for any reason the background cycling/activity of the RNG is interrupted, the next seed value for the RNG must be a function of the value produced by the RNG immediately prior to the interruption.

6.3.7 Winning Number Draw

a) The winning number selection shall only be produced from sold draw numbers for the current drawing to be available for selection.
b) Each valid, sold raffle number shall be available for random selection at the initiation of each drawing.
c) For raffles which offer multiple awards or drawings with separate buy-ins for each, the winning number selection shall only be produced from sold draw numbers corresponding with each applicable award or drawing. As winning numbers are drawn, they shall be immediately used as governed by the rules of the raffle (i.e. the counterfoils are not to be discarded due to adaptive behavior).

6.3.8 Scaling Algorithms

The methods of scaling (i.e. converting raw RNG outcomes of a greater range into scaled RNG outcomes of a lesser range) must be linear, and must not introduce any bias, pattern or

predictability. The scaled RNG outcomes must be proven to pass various recognized statistical tests.

a) If a random number with a range shorter than that provided by the RNG is required for some purpose within the raffle system, 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.