Technical Gaming Standards for Electronic Raffle Systems

Electronic Raffle Standards Document (ERSD)
Version 1.0

AGLC
Choices Albertans can trust.

Revision Date: July 2018

Date	Revised Section	Version #

Revision History

Contents

Section 1: Introduction

The objective of this document is to ensure that Electronic Raffle Systems operating in Alberta are secure and operated with integrity. This Electronic Raffle Standards Document (ERSD) outlines the minimum technical standards for approval of ERSs in Alberta.

From time to time, the AGLC will review this ERSD and incorporate any additional applicable minimum standards as required. In recognition that technology and raffle products will evolve, suppliers are encouraged to contact the AGLC to discuss proposed technology or game designs and how their proposals may comply with the intent of these standards.

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

a) Gaming Laboratories International Standard (GLI-31) - Standards for Electronic Raffle Systems (ERS).

b) British Columbia Gaming Policy and Enforcement Branch (GPEB) - Technical Gaming Standards for Electronic Raffle Systems (TGS6) and for Internet Gaming Systems (TGS5).

c) Saskatchewan Liquor and Gaming Authority - Standards for On-line Raffle Ticket Sales.

d) Liquor and Gaming Authority of Manitoba – Technical Standards for Electronic Raffle Systems.

The purpose of this ERSD is as follows:

a) To eliminate subjective criteria in analyzing and certifying Electronic Raffle System operation.

b) To only test those criteria which impact the credibility and integrity of Electronic Raffle Systems operation from both the Revenue Collection and Player’s game play point of view.

c) To create an ERSD that will help ensure that Electronic Raffle Systems operating in the live environment are fair, secure, safe, auditable, operating correctly and with integrity.

d) To recognize that testing which does not impact the credibility and integrity of the Electronic Raffle System (such as electrical testing) must not be incorporated into this ERSD but left to appropriate test laboratories that specialize in this type of testing.

e) To recognize that except where specifically identified in this ERSD, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer of the equipment.

f) To construct an ERSD that can be easily changed or modified to allow for new technology or functionality.

g) To construct an ERSD 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 ERSD, while at the same time, to encourage new methods and technologies to be developed.

1.1 – Legislation and Regulation

1.1.1 The following legislation and regulation will take precedence over this ERSD:

a) the *Criminal Code* (Canada);

b) the Alberta *Gaming and Liquor Act*; and

c) the Alberta Gaming and Liquor Regulation

1.2 – Definitions

1.2.1 In this Handbook:

a) "access control" means the restriction of access to a place or other resource, such as locks and login credentials.

b) "accredited testing facility" (or ATF) means a test facility or laboratory registered and approved by the AGLC for the purpose of gaming supply testing and certification.

c) "address resolution protocol" (ARP) means the protocol used to translate IP addresses into MAC addresses to support communication on a LAN (Local Area Network).

d) "AGLC" means the Alberta Gaming and Liquor Commission.

e) "algorithm" means a finite set of unambiguous instructions performed in a prescribed sequence (mathematical rule or procedure) used to compute a desired result.

f) "authentication" means 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.

g) "bearer ticket" means a ticket without the buyer's name, address, or telephone number.

h) "bi-directional" means the ability to move, transfer, or transmit data in both directions.

i) "counterfoil" means a paper or electronic entry containing a ticket number matching the player's purchased ticket that will be used to conduct a draw (includes ticket stub).

j) "critical memory" means memory that is used to store all data that is considered vital to the continued operation of the raffle.

k) "cryptographic" means anything written in a secret code, cipher, or the like.

l) "distributed denial of service" (DDoS) means a type of DoS attack where multiple compromised systems are used to target a single system causing temporary interruption or suspension of the services of a host.

m) "draw" means the approved random selection process by which the raffle winner(s) is determined.

n) “domain” means a group of computers and devices on a network that are administered as a unit with common rules and procedures.

o) “electronic bearer ticket raffle” means a raffle conducted during a specific sports or entertainment event, where the charitable organization sells and prints tickets using a Raffle Sales Unit and conducts the draw on the same day the tickets were sold.

p) “electronic draw” means a draw to determine a prize winner using ATF certified and AGLC approved computer software that utilizes a random number generator (RNG).

q) “electronic entry” means the electronic record of a purchased raffle ticket that is entered into a draw to be conducted with a random number generator.

r) “electronic raffle system” (or ERS) means ATF certified and AGLC approved computer proprietary software and applicable proprietary hardware that provides, based on eligibility criteria, electronic raffle components for licensed charitable organizations to conduct either an electronic traditional ticket raffle or an electronic bearer ticket raffle resulting in either a paper or electronic draw.

s) “electronic traditional ticket raffle” means a raffle using an electronic raffle system and where the charitable organization sells tickets for a period of time prior to the raffle draw.

t) “encryption” means the reversible transformation of data from the original (plaintext) to a difficult-to-interpret format (ciphertext) as a mechanism for protecting its confidentiality, integrity, and sometimes its authenticity.

u) “encryption key” means a sequence of characters used to encrypt or decrypt data.

v) “firewall” means any number of security schemes that prevent unauthorized communication to and from a network.

w) “gaming supplier” means an individual, corporation or other entity that makes, sells, advertises or distributes gaming supplies either directly or indirectly to a licensed charitable organization in Alberta pursuant to section 40(1)(a) of the *Gaming and Liquor Act*.

x) “geolocation” means identifying the real-world geographic location of an Internet connected computer, mobile device, or website visitor.

y) “host” means a computer or other device connected to a network that offers information, services, or applications to the network.

z) “hypertext transfer protocol” (HTTP) means the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers must take in response to various commands.

aa) “Internet” means an interconnected system of networks that connects computers around the world via the TCP/IP protocol.

bb) “intrusion detection system (IDS)/intrusion prevention system (IPS)” means the process of monitoring computer and network activities, and analyzing those events to look for signs of intrusion in the system.

cc) “IP address” means Internet Protocol address, an identifier for a computer or device on a TCP/IP network.

dd) “MAC address” means Media Access Control address, a hexadecimal sequence, embedded in all communication hardware, which can uniquely identify any device on a network.

ee) “man-in-the-middle” (MITM) means an active Internet attack where the person attacking attempts to intercept, read, or alter information moving between two computers.

ff) “message authentication” means a short piece of imbedded code used to prove the integrity and authenticity of a transmission packet.

gg) “online” means anything that is connected to the Internet.

hh) “online ticket distribution” means an ATF certified and AGLC approved computer software platform used to send a ticket to the purchaser through the Internet, where the purchaser downloads a copy of the ticket.

ii) “online ticket ordering” means a computer software platform that only receives ticket orders through the Internet and that may process payments in real time. The charitable organization handles the ticket order(s) prior to providing the raffle ticket to the purchaser, e.g. processing the payment, confirming receipt of payment, confirming order details.

jj) “online ticket sales” means an ATF certified and AGLC approved computer software platform which fully automates all aspects of a ticket purchase through the Internet including ticket ordering, processing of payments in real time and provision of the ticket to the player. The charitable organization does not handle the ticket order(s) prior to providing the raffle ticket to the purchaser.

kk) “proprietary equipment” means equipment designed and/or distributed by a gaming supplier for a specific purpose or use as a gaming supply in connection with an ERS.

ll) “proprietary software” means software designed and/or distributed by a gaming supplier for a specific purpose or use as a gaming supply in connection with an ERS.

mm) “protocol communication” means a set of formal rules describing how to exchange data across a network.

nn) “raffle event” means a full lifecycle from the setup of the raffle on the system through sales and winner selection and final closure of the system.

oo) “raffle sales units” (RSU) means an ATF certified and AGLC approved portable/wireless device, a remote hard-wired connected device, or standalone cashier station that is used as a point of sale for bearer tickets.

pp) “random number generator (or RNG)” means an ATF certified and AGLC approved computer software designed to generate a sequence of numbers that cannot be reasonably predicted. An RNG is used to conduct an random electronic draw to determine the outcome(s) of the raffle.

qq) “remote access” means any access from outside the system or system network including any access from other networks within the establishment.

rr) “security certificate” means information often stored as a text file and is used by the SSL (Secure Socket Layers) Protocol to establish a secure connection; both sides must have a valid Security Certificate, which may also be called a Digital ID.

ss) “seeding or re-seeding” means the method of determining the initiating value (seed) to be used by the random number generator algorithm.

tt) “server” means a running instance of software that is capable of accepting requests from clients, and the computer that executes such software. Servers operate within a Client-Server Architecture, in which “servers” are computer programs running to serve the requests of other programs (clients).

uu) “shellcode” means a small piece of code used as the payload (cargo of data transmission) in the exploitation of computer security. Shellcode exploits vulnerability and allows an attacker the ability to reduce a computer system’s information assurance.

vv) “significant event” means any event that impacts the operation, security, or integrity of the ERS and/or the outcome of the raffle.

ww) “stateless protocol” means a communications scheme that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.

xx) “transmission control protocol (TCP)/Internet protocol (IP)” means the suite of communications protocols used to connect hosts on the Internet.

yy) “ticket” means a paper or electronic record provided to a ticket purchaser for an electronic bearer ticket raffle or an electronic traditional ticket raffle.

zz) “ticket number” means a uniquely identifiable number that is provided to the purchaser for each draw entry purchased, and is eligible to be selected as the winning number for the raffle.

aaa) “website/site” means a set of related web pages typically served from a single web domain.

bbb) “world wide web/web” – means a hypertext system that operates over the Internet.

Section 2: General

2.1 – General Statements

2.1.1 Before operating, each Electronic Raffle System (ERS) used in Alberta must be presented to the AGLC for approval. The AGLC will determine if these gaming supplies require testing to the standards set forth in the ERSD:

a) The ERSD may apply in part or in whole to an ERS proposed for use in the conduct of a raffle.

b) A gaming supplier may select an AGLC registered Accredited Testing Facility (ATF) to perform the required testing.

c) The gaming supplier must ensure that the ATF provides the final test results, reports, any additional documentation or discussion directly to the AGLC.

d) A licensed group proposing to use an ERS not obtained from a gaming supplier (developed by the licensed group) may select an AGLC approved ATF to perform the required testing.

e) A licensed group proposing to use an ERS not obtained from a gaming supplier (developed by the licensed group) must ensure that the ATF provides the final test results, reports, and any additional documentation or discussion to the AGLC.

f) Although the ATF may recommend the approval of gaming supplies for use in Alberta, the ultimate authority to approve gaming supplies rests solely with the AGLC.

2.1.2 The ERS must be identified in the ATF certification as being capable of conducting an electronic traditional ticket raffle and/or an electronic bearer ticket raffle respecting the electronic components as follows:

a) An ERS for electronic traditional ticket raffle includes the use of electronic components as follows:

i. online ticket ordering in combination with online ticket distribution and/or an electronic draw; or

ii. online ticket sales; or

iii. online ticket sales in combination with online ticket distribution and/or an electronic draw.

b) An ERS for electronic bearer ticket raffles includes the use of electronic components as follows:

i. the sale of tickets using raffle sales units (RSUs); or

ii. the sale of tickets using raffles sales units (RSUs) with an electronic draw.

2.1.3 The ERS must have operation and service manuals directly related to the system used to sell raffle tickets; these manuals must be provided to the AGLC. The following manuals and documents are required:

a) operation manuals for the ERS; and

b) technical service manuals which:

i. depict the system for which the manual is intended to cover;

ii. provide adequate detail and diagrams to support interpretation by the AGLC;

iii. include a maintenance schedule outlining the elements of the ERS that require maintenance and the frequency at which the maintenance must be carried out;

iv. include a maintenance checklist that enables 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.

2.1.4 The AGLC will determine if an ERS is to be certified in two phases:

a) The ATF will test the integrity of the system in conjunction with the supplied RSUs, in a laboratory setting with the equipment assembled.

b) On-site testing following the initial install of the system to ensure proper configuration of the security applications. 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 the AGLC.

2.1.5 An ATF must provide the AGLC with a mechanism to ensure all file scripts within the ERS have not been altered after the ATF has approved the ERS.

2.1.6 In addition to the requirements in this Electronic Raffles Standards Document, gaming suppliers must comply with the Gaming and Liquor Act, the Gaming and Liquor Regulation, Board policies including the Electronic Raffle Handbook, and the terms and conditions of registration. Failure to do so may result in disciplinary action up to and including the suspension or cancellation of the registration (see Subsection 10.1.15 in the Electronic Raffle Handbook).

Section 3: Electronic Raffle Systems Management

3.1 – General ERS Operating Procedures

3.1.1 **Prize and Ticket Limitations –** An ERS must be capable of configuring limits for the maximum prize amount that may be won and the maximum number of tickets to be sold.

3.1.2 **Time Limits –** An ERS must be capable of setting time limits for when tickets may be purchased for a raffle draw. This includes setting a time limit for closing sales and terminating the draw.

3.1.3 **System Configuration Changes** – The ERS, through a software lock, must ensure that once a raffle has commenced, system configuration changes are not permitted until the completion of the raffle. Any changes needed to be made to the raffle settings as administered by the ERS is allowed with prior approval from the AGLC, the system must record any changes to the raffle settings in an event log.

3.1.4 **Software Changes –** After the commencement of a raffle, the ERS software must not allow changes that could affect the integrity of the raffle. Any changes require prior approval from the AGLC.

3.1.5 **Ticket Purchaser Information –** the ERS must employ a mechanism to securely collect information required to complete a sale from a purchaser. Once the identity verification is completed, and the purchaser has acknowledged all of the necessary privacy policies and the terms and conditions, the ticket may be purchased (See Section 5.1.17).

3.1.6 **Account Registration –** the ERS must employ a mechanism to securely collect information required to complete registration of a purchaser account. Once the identity verification is completed, and the purchaser has acknowledged all of the necessary privacy policies and the terms and conditions, the purchaser account can become active. The purchaser must be fully registered and their account must be activated prior to permitting ticket purchases.

3.1.7 **Geolocation –** the ERS or online purchasing platform must be able to reasonably detect the physical location of an authorized patron attempting to access the service. Third parties may be used to verify the location of patrons as allowed by the AGLC.

3.2 – Tickets and Entries for Traditional Ticket Raffles

3.2.1 **ERS Ticket Generation** – An ERS must:

a) be capable of generating a ticket online, with one or more uniquely identifiable ticket number(s);

b) not generate duplicate ticket numbers within the same event;

c) only generate tickets and entries for the current raffle;

d) only generate tickets after payment has been processed;

e) not generate additional entries for ticket reprints or redistribution of online tickets; and

f) generate ticket numbers with only one matching counterfoil.

3.2.2 **Online Distribution of Tickets and Sales Receipts** – Tickets and sales receipt may be issued online once payment has been processed.

3.2.3 **Raffle Ticket Information** – A raffle ticket must be issued with the following information, at minimum:

a) the licensed group's name and address;

b) the raffle licence number;

c) ticket number;

d) barcode (optional);

e) ticket price;

f) total number of tickets to be sold;

g) issued date and time in 24 hour format showing hours and minutes;

h) location(s) and date(s) of the draw;

i) description and value of prize(s);

j) the notice: "Restrictions apply to prizes" (if applicable);

k) cash alternatives (if applicable); and

l) the notice: "Must be at least 18 years of age to purchase".

3.2.4 **Additional Information on Tickets** – It is permissible for the raffle ticket to contain additional information such as advertising, logos, and coupons. This information may be contained on the ticket itself; however, this information must not impact or obscure the required information.

3.2.5 **Ticket Differentiation** – Where a series of raffles are conducted by a licensed charity, tickets for each raffle must be differentiated from the other tickets used in the series.

3.2.6 **Discount Tickets** – The ERS may sell multiple tickets for a discounted price (for example, three for $5). A unique series number must be printed on each discounted ticket, corresponding to the price group from which the discounted ticket was purchased [for example, For single tickets priced at $2 each "Series A (ticket number)" and for tickets priced at three for $5 "Series B (ticket number)"].

3.2.7 **Single Tickets** – The ERS must always be capable of processing single ticket purchases.

3.2.8 **Counterfoils -** The ERS must generate a unique counterfoil for each ticket number. A counterfoil must be printed or entered electronically according to the type of draw to be conducted. Printed counterfoils must be the same size, shape, and weight. All counterfoils must have an equal chance of being selected. Counterfoils must include the following information, at a minimum:

a) the name, address, and telephone number of the ticket purchaser provided during the online purchase;

b) license number;

c) ticket number;

d) issued date and time in 24 hour format showing hours and minutes; and

e) an optional barcode.

3.2.9 **Ticket Numbers –** The ERS must generate ticket numbers consecutively.

3.2.10 **Voiding a Ticket -** the ERS must have the capability to void a ticket and flag or otherwise identify a voided ticket and its corresponding ticket number(s). The ERS must record, at a minimum, the ticket numbers and the ticket number from the voided ticket. Voided ticket numbers must not be able to be resold or reissued for that raffle. The ERS must automatically adjust the total sales figure when a ticket is voided.

3.3 – Raffle Displays

3.3.1 **Jackpot Displays (Bearer Ticket Draws) –** An ERS that supports a raffle prize display, intended to be viewed by participants of the raffle, must indicate the raffle prize as the dollar amount that may be won.

3.3.2 **Winning Ticket Number Display (Traditional Ticket Raffles) –** An ERS that supports a display of the winning ticket number must display the winning number in the same format as it appears on the ticket.

3.4 – Closing Sales and Reconciliation

3.4.1 **General Statement** – A raffle draw, with the exception of early bird draws (See 3.4.2), may only be concluded after:

a) the close of the raffle; and

b) all sales and voided sales for the raffle purchase period have been reconciled.

3.4.2 **Early Bird Draws** – If an ERS is capable of conducting an early bird draw(s), the ERS must be capable of reconciling ticket sales to verify all tickets sold prior to the early bird draw date(s) are accounted for and eligible for selection in the draw.

3.4.3 **Closing the Raffle Period** – The ERS must be capable of closing off the sale of raffle tickets at a time determined by the operator. No sale of tickets may occur after the raffle purchase period has closed. The ERS must be capable of notifying that all ticket sales have been uploaded, transferred, or otherwise communicated to the server.

3.4.4 **Time and Ticket Counter Display** – The ERS must be capable of displaying the amount of tickets remaining before sales close. Once closed, the display must indicate that sales have closed.

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

3.5 – Winner Determination

3.5.1 **Winner Verification** – The ERS must be capable of verifying the winning ticket. Winning bearer tickets may be verified either manually or through a barcode. Winning tickets for a traditional ticket raffle may be verified through a barcode, purchaser information, or ticket number. Winning tickets must be verified prior to payout; once verified, the ERS must record and retain the winning number with the system database.

3.5.2 **Official Draw Results** – Results of the draw become official and final after the winning ticket is verified and provided to the licensed group. The system must display the winning draw on all capable display devices intended to be viewed by participants.

3.5.3 **Multiple Prize Draws** – An ERS conducting an electronic draw with ticket numbers eligible for multiple prizes must be capable of re-entering the previously drawn ticket numbers for non-identical prizes. The ERS may be configured to remove a ticket number from selection once it is drawn if the subsequent draw(s) are for an identical prize. All eligible tickets must be available for selection for the grand prize.

3.6 – Accounting and Reporting

3.6.1 **General Statement** – The ERS must be capable of producing general accounting and exception reports. These reports must be run, reviewed, verified, and retained after the completion of each raffle.

3.6.2 **Reporting Requirements** – The ERS must be capable of producing general accounting and exception reports to include the following information for each concluded draw:

a) raffle draw report, including the following information:
   i. date and time of event;
   ii. date and time of the start and finish of sales;
   iii. licensee identification;
   iv. sales information (sales totals, refunds, voids, reprints, misprints, and sales by price point);
   v. prize(s) awarded to winning participant(s);
   vi. refund totals by event;
   vii. ticket numbers-in-play count;
   viii. order in which the winning tickets were drawn;
   ix. winning number drawn; and
   x. other reports as requested by the AGLC.

b) Error/Exception Report – A report outlining system exception information including, but not limited to, changes to system parameters, corrections, overrides, and voids. All error/exception reports must include date and time stamp of the event(s).

c) Ticket Report – A report which includes a list of all tickets sold, including all associated ticket numbers, selling price, and RSU identifier.

d) Sales by RSU – A report including the breakdown of each RSU's total sales (including ticket numbers) and any voided, and misprinted tickets.

e) Sales online – A report including a breakdown of online sales, including ticket numbers issued and any voided or reissue requests.

f) Voided Ticket Number Report – A report which lists all ticket numbers that have been voided.

g) RSU Event Log – A report listing all events recorded for each RSU, including the date and time, and a brief text description of the event and/or identifying code.

h) Reconciliation Report – A report detailing tickets sold online, over the telephone, and/or in-person.

i) RSU Corruption Log – A report listing all RSUs that are unable to be reconciled to the system, including the RSU identifier, RSU operator, and the money collected.

j) Online Corruption Log – A report listing all online transactions that were unable to be reconciled to the system.

Section 4: Bearer Ticket Draws

4.1 – Raffle Sales Unit Types

4.1.1 **General Statement –** All RSUs must be controlled by the charity. After the payment of a fee, participants receive a bearer draw ticket. A chance to win may be purchased either from an attendant-operated RSU or a player-operated RSU. Any other methods will be reviewed by the AGLC on a case-by-case basis.

4.1.2 **Attendant-Operated Raffle Sales Unit** – A participant may purchase a bearer ticket from an attendant-operated RSU by providing payment for the ticket(s) to the attendant. Upon receiving payment, the attendant will provide the purchased bearer ticket(s) to the participant.

4.1.3 **Player Operated Raffle Sales Unit –** A participant may purchase a bearer ticket from a player-operated RSU by following the instructions appearing on the screen of the RSU and providing payment for the ticket(s). Upon payment, the RSU will issue the corresponding bearer ticket(s) to the participant.

4.2 – Raffle Sales Unit Operations and Security

4.2.1 **General Statement –** An ERS must have 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 ERS and generates a counterfoil into a draw.

4.2.2 **Additional Information on Tickets** – It is permissible that a ticket may contain additional printed information such as advertising, logos, and coupons. Some of this information may be contained on the ticket stock itself. Any additional printed information must not impact or obscure the required printed information. It is not recommended that counterfoils or electronic entries contain any additional printed information.

4.2.3 **Ticket Printing** – An RSU must be capable of generating and printing a bearer ticket with one or more uniquely identifiable ticket numbers.

4.2.4 **Duplicate Ticket Numbers** – The ERS must not generate duplicate ticket numbers within the same event. For each ticket number generated, there must be only one corresponding counterfoil with that ticket number.

4.2.5 **Discount Tickets** – The ERS may sell multiple tickets for a discounted price (for example, 3 for $5). A unique series number must be printed on each discounted ticket, corresponding to the price group from which the discounted ticket was purchased.

4.2.6 **Single Tickets** – The RSU must always be capable of processing single ticket purchases.

4.2.7 **Transaction Receipt** – The RSU must be capable of providing a transaction receipt in the form of a bearer ticket to a purchaser.

4.2.8 **Access Controls** – Access to raffle sales software must be controlled by a secure logon procedure. It must not be possible to modify the configuration settings of the RSU without an authorized logon.

4.2.9 **Touch Screens** – Touch screens must be accurate once calibrated. This accuracy must be maintained for at least the manufacturer's recommended maintenance period.

4.2.10 **Interface** – The functions of all buttons, touch or click points represented on the RSU interface must be clearly indicated within the area of the button, or touch/click point and/or touch/click points on the RSU that are undocumented.

4.2.11 **Communications** – An RSU must only communicate with authorized ERS components. The ERS must have the capability to uniquely identify and authorize each RSU to be used to sell tickets.

4.2.12 **Wireless RSUs** – Communication must only occur between the RSU and the ERS via authorized access points.

4.3 – Bearer Ticket Printers

4.3.1 **Printing Bearer Tickets** – If the RSU connects to a printer that is used to produce bearer tickets, the ticket must include information as required in section 4.3 of the Electronic Raffle Handbook. This information may be included on the ticket stock itself.

4.3.2 **Data Sent to Printers** – The RSU must control the transfer of ticket data sent to the printer, and only transfer ticket data to the printer when sufficient space is available in the printer memory to receive the ticket information.

4.3.3 **Use of Barcodes** – If a barcode forms part of the ticket number printed on the bearer ticket, the printer must support the barcode format and print with sufficient resolution to permit validation by a barcode reader.

4.3.4 **Printer Error Conditions** – The bearer ticket printer must be able to detect and indicate to the operator the following error conditions:

a) low battery;

b) out of paper or low paper;

c) printer disconnected; and

d) if the unit is capable of reprinting a ticket, the reprinted ticket must clearly indicate that it is a reprint of the original ticket.

4.4 – Critical Memory Requirements

4.4.1 **Definition of Critical Memory –** Critical memory is used to store all data that is considered vital to the continued operation of the RSU. Critical memory must be maintained for the purpose of storing and preserving critical data. Critical memory may be maintained by any component(s) of the ERS. This includes, but is not limited to:

a) when not communicating with the system, recall of all tickets sold including ticket numbers; and

b) RSU configuration data.

4.4.2 **Maintenance of Critical Memory** – Critical memory storage must be maintained in such a way that enables errors to be identified. This may involve signatures, checksums, multiple copies, time stamps, and/or effective use of validity codes.

4.4.3 **Comprehensive Checks** – Comprehensive checks of critical memory must be made on start-up and must detect failures with an extremely high level of accuracy.

4.4.4 **Unrecoverable Critical Memory** – An unrecoverable corruption of critical memory must result in an error. Upon detection, the RSU must cease to function.

4.4.5 **Backup Requirements** – The RSU must have a backup to archive capability, which allows the recovery of critical data, should a failure occur.

4.5 – Program Requirements

4.5.1 **Identification** – All programs must contain sufficient information to identify the software and revision level of the information stored on the RSU, which may be displayed via a display screen. The process used in the identification of the software and revision level will be evaluated on a case-by-case basis by the ATF.

4.5.2 **Detection of Corruption** – RSU programs must be capable of detecting program corruption and cause the RSU to cease operations until corrected. Program verification mechanisms will be evaluated on a case-by-case basis by the ATF based on industry-standard security practices.

4.5.3 **Verification of Updates** – Prior to execution of the updated software, the software must be authenticated on the RSU.

4.6 – Independent Control Program Verification

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

4.7 – Tickets and Entries

4.7.1 **ERS Ticket Generation –** The ERS must:

a) be capable of generating and printing, via the RSU, a ticket with one or more uniquely identifiable ticket number(s);

b) not generate duplicate ticket numbers within the same event;

c) only generate tickets and entries for the current raffle;

d) not generate additional entries for ticket reprints or redistribution of online tickets; and

e) generate ticket numbers with only one matching counterfoil.

4.7.2 **Bearer Tickets –** After the payment of a fee, participants receive a bearer ticket for one or more chances to win a raffle draw. The bearer ticket must be printed with the following information:

a) name of organization conducting the raffle;
b) event location;
c) RSU identifier from which the ticket was generated;
d) unique ticket number(s) and optional barcode;
e) licence number;
f) ticket number;
g) issued date and time (in 24 hour format showing hours and minutes); and
h) value or cost of the bearer ticket.

Note: If a series of draws are conducted on a single day, the tickets sold for each draw must be uniquely identifiable from tickets sold for other draws conducted on the same day. For example, this may be achieved through a different event identifier.

4.7.3 **Ticket Numbers –** The ERS must generate ticket numbers consecutively.

4.7.4 **Voiding a Ticket –** The electronic raffle system must flag or otherwise identify a voided bearer ticket and its corresponding ticket number(s). The system must record the ticket numbers from the voided bearer ticket. Voided ticket numbers shall not be able to be resold or reissued for that raffle.

4.7.5 **Additional Printed Information –** It is permissible that a bearer ticket may contain additional printed information such as advertising, logos, and coupons. Some of this information may be contained on the ticket stock itself. Any additional printed information must not impact or obscure the required printed information.

4.7.6 **Counterfoils –** The ERS must generate a unique counterfoil for each ticket number. A counterfoil must be printed or entered electronically according to the type of draw to be conducted. Printed counterfoils must be the same size, shape, and weight. All counterfoils must have an equal chance of being selected. Counterfoils must include the following information, at a minimum:

a) event location;
b) licence number;
c) issued date and time (in 24 hour format showing hours and minutes);
d) value or cost of the bearer ticket; and
e) unique ticket number and optional barcode.

4.7.7 **Printed Counterfoils –** If an RNG is used to determine the winner of the raffle, a printed counterfoil is not required.

4.7.8 **Reprinting of Counterfoils –** Where the system supports the reprinting of counterfoils, this facility must require additional supervised access controls, such as a password, and the ticket numbers must be flagged in the system as reprints.

4.7.9 **Closure of RSUs** – The ERS must be capable of displaying to the licensee by way of the RSU device display that all sales within a particular RSU have been uploaded, transferred, or otherwise communicated to the ERS:

a) on verification of the sales data transfer, the RSU device must be capable of being reset or closed; and
b) the RSU must not permit any additional sales for the current raffle once closed.

4.7.10 **Reconciliation** – the ERS must be capable of reconciling all sales, at a time determined by the operator, including sold, unsold, and voided sales for the raffle purchase period to ensure that only valid ticket numbers are eligible to win. No sales of tickets may occur after the raffle purchase period has been closed.

4.8– RSU Management Requirements

4.8.1 **RSU Management Functionality –** An ERS must have a master list of each authorized RSU in operation, including (at minimum) the following information for each counterfoil. If the following parameters can be retrieved directly from the RSU, controls must be in place to ensure accuracy of the information:

a) a unique RSU identification number or corresponding hardware identifier, such as a MAC;

b) operator identification; and

c) tickets issued for sale, if applicable.

4.8.2 **RSU Validation -** It is recommended that RSUs be validated at pre-defined time intervals with at least one method of authentication. This time interval must be configurable and can be set to a maximum value of 60 minutes. The system must have the ability to remotely disable the RSU after the threshold of unsuccessful validation attempts has been reached.

Section 5: The Electronic Raffle System Platform

5.1 – Operation & Server Security

5.1.1 **General Statement –** The ERS server(s) must be located within the province of Alberta. Remote location through a Wide Area Network (WAN) of the platform server will require prior approval of the AGLC. Backups and recovery files may be located on secure media within Canada.

5.1.2 **Logical Access –** The ERS must be capable of logically securing access using generally accepted practices for IT network security, which may include but is not limited to, the following technologies:

a) passwords;

b) PINS;

c) biometrics; or

d) authentication credentials (e.g.: magnetic swipe, proximity cards, embedded chip cards).

5.1.3 **ERS Security Access Levels –** The ERS must have multiple security access levels to control and restrict different classes of access to the system.

5.1.4 **ERS Access Controls –** Access privileges must be restricted and controlled:

a) a user registration and de-registration procedure must be in place for granting and revoking access to all information systems and services;

b) all users must have a unique user ID for their personal use only, and an authentication technique must be chosen to substantiate the claimed identity of the user;

c) generic accounts are permitted; however, their use must be limited to simple functionality and use must be formally documented and submitted to AGLC for approval;

d) password provision must be controlled through a formal management process, and must meet requirements for length, complexity, and lifespan;

e) access to system applications must be controlled by a secure log-on procedure;

f) any physical or logical access to the areas housing components or applications used for the sale of raffle tickets through remote access means must create a log entry for security review;

g) the use of automated equipment identification to authenticate connections from specific locations and equipment must be maintained in a report;

h) restrictions on connection times must be used to provide additional security for high-risk applications;

i) the use of utility programs that might be capable of overriding system application controls must be restricted and controlled; and

j) a formal policy must be in place and appropriate security measures adopted to protect against the risks of using mobile computing and communication facilities.

5.1.5 **Security from Alteration or Tampering –** The ERS must provide a logical means for securing the raffle data against alteration, tampering, or unauthorized access. To that end, the following requirements also apply to the ERS:

a) ERS equipment must have a mechanism whereby an error will not cause the raffle data to automatically clear. Data must be maintained at all times regardless of whether the server is being supplied with power.

b) data must be stored in a manner that prevents the loss of data when replacing parts or modules during maintenance.

5.1.6 **Data Alteration –** The ERS must not permit alteration of any accounting, reporting, or significant event data without supervised access controls. In the event any data is changed, the changed data must be available in a log file or report with the following details:

a) data element that was 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's login.

5.1.7 **Server Programming –** The ERS platform must not allow the user(s) to conduct programming on the server that may result in modifications to the ERS application. It is acceptable for an authorized network administrator to perform specified network infrastructure maintenance or troubleshooting.

5.1.8 **Virus Protection –** The ERS must have virus protection software.

5.1.9 **Copy Protection –** Copy protection to prevent unauthorized duplication or modification of the ERS software must be provided. The method of copy protection must be fully documented and verified by the ATF.

5.1.10 **System Clock –** An ERS must maintain an internal 24-hour clock that synchronizes with all other system clocks, reflecting the current date and time. The system clock must be used to provide the following:

a) a time stamp of significant events.;

b) a reference clock for reporting; and

c) time stamping of all sales and draw events.

5.1.11 **System Clock Synchronization –** if multiple clocks are supported, the system must have the ability to synchronize clocks within the ERS.

5.1.12 **Printer Error Conditions –** Where printed counterfoils are in use, the printer mechanism must be able to detect and indicate the following conditions:

a) out of paper – the system must detect (alert) this error condition when it tries to print;

b) paper low – there must be a means for the attendant to be alerted;

c) buffer overrun;

d) printer jam/failure;

e) memory error;

f) printer failure; and

g) printer disconnected.

5.1.13 **Printer Specifications –** All printers used in the platform must be capable of printing entries in the format laid out in this ERSD.

5.1.14 **Printer Configuration -** The design of physical layouts of the printers must ensure that all printed entries are available to be drawn using the manual draw process as specified on the raffle licence. With the exception of paper roll changes, the printer must not rely on any operator intervention to ensure that every printed counterfoil is collected.

5.1.15 **Low Printer Paper –** All printers must have the ability to detect a low paper condition and create an alert for the attendant. At no time must a printer be available to the system to print a counterfoil if it is without paper. Upon detection of a low paper condition:

a) the printer must have the capacity to complete the current print request;

b) the printer must not accept any further print requests and will remain unavailable until additional paper has been added; and

c) on resolution, the printer must become available to the system without requiring an operator to reconfigure the printer settings.

5.1.16 **Disabling the Printer –** 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.

5.1.17 **ERS Payment Processor –** An ERS may contain or employ a 3rd party payment processor or associated API to conduct ticket sales. This payment processor must meet all current PCI Security Standards Council requirements. Where a payment processor is used the ERS cannot retain the information collected by the payment processor application. This includes bank account information, credit card numbers, and card verification value (CVV) numbers. The ERS may retain the purchaser's name, address, phone number, and email address for verification and contact purposes.

5.2 – Significant Events

5.2.1 **Event Logging –** Significant events must be communicated and logged on the ERS. Once generated, event logs may not be altered. Event logs must include:

a) connection or disconnection of an RSU or any component of the system;

b) critical memory corruption of any component of the system;

c) printer errors for raffle entries, including:

i. low paper or out of paper;

ii. printer disconnect or failure; and

iii. printer memory error.

d) establishment and failure of communications between sensitive ERS components;

e) significant event buffer full;

f) program error or authentication mismatch;

g) firewall audit log full (where supported);

h) remove access (where supported);

i) RSU event log;

j) RSU corruption log; and

k) any other significant events.

5.2.2 **Surveillance and Security Functionality –** An ERS must provide an interrogation program that enables an online comprehensive searching of the significant events log. The interrogation program must have the ability to perform a search using one or more of the following criteria:

a) data and time range;
b) unique component identification number; and
c) the ability to filter by significant event identifier.

5.3 – Backups and Security

5.3.1 **Storage Medium Backup –** The ERS must 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 must be kept on the ERS with open support for backups and restoration:

a) all storage of critical data must use error checking and must be stored on a non-volatile physical medium;
b) the ERS must have the ability to perform backups, including physical location of medium storage. Procedures for periodic testing recovery must be provided to the AGLC as a condition of equipment approval; and
c) the database must be stored on redundant media so that no single failure of any portion of the system would cause the loss or corruption of data.

5.3.2 **Recovery Requirements –** In the event of a catastrophic failure when the ERS cannot be restored 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 files or raffle set-up.

5.4 – System Software

5.4.1 **Verification of System Software –** Software components and modules must be verifiable by a secure means at the system level, denoting Program ID and version. The system must 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. This must be accomplished by being authenticated by a third-party device, or by allowing for removal of the media such that it can be verified externally. Other methods may be evaluated by the ATF on a case-by-case basis. This integrity check will provide a means for field verification of the system components and modules to identify and validate the programs or files. The ATF, prior to system approval, must approve the integrity check method.

5.4.2 **Regulator's Portal –** Where the ERS server is located off-site of the raffle event or an RNG is being used to conduct an electronic draw, the ERS must allow for the verification of server files remotely. The method of logging in and obtaining the required information in 5.4.1 must be provided to the AGLC.

Section 6: Communication and Connectivity Requirements

6.1 – Communication and Connectivity

6.1.1 **Connections –** An ERS may use various methods of communication, and may include:

a) Ethernet connections;

b) wireless communications protocol commonly known as 802.11(x);

c) Bluetooth; and

d) cellular.

6.1.2 **Communication Protocol –** Each component of an ERS must function as indicated by the communication protocol implemented. An ERS must provide for the following:

a) Communication between all system components that must provide mutual authentication between the ERS component and the server;

b) Protocols must use communication techniques that have proper error detection and recovery mechanisms, designed to prevent eavesdropping and tampering. Any alternative implementation will be reviewed on a case-by- case basis by the ATF, with approval of the AGLC;

c) All communications critical to the raffle must be encrypted. The encryption must employ variable keys, or similar methodology to preserve secure communication;

d) Personally identifiable information, sensitive account data, and financial information must be protected over a public network;

e) Sufficient redundancy and the ability to backup and restore copies of critical data in order to recover and continue with the raffle. Backup copies must include items required in the event of a catastrophic failure and include:

i. significant event information;

ii. accounting information;

iii. reporting information;

iv. specific site information;

v. user/employee files; and

vi. raffle setup.

f) An intrusion detection system/intrusion prevention system must be installed on the network, which can (at minimum):

i. listen to both internal and external network activities;

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;

v. detect other man-in-the-middle indicators;

vi. stateless protocols, such as UDP, must not be used for sensitive data without stateful transport. Although HTTP is stateless, it is permitted if run on TCP;

vii. all changes to network infrastructure, such as network device configuration, must be logged;

viii. virus scanners and/or detection programs must be installed on all pertinent information systems. These programs must be updated regularly to scan for new types of viruses;

ix. network security should be tested by a qualified and experienced individual, and may be required at the request of the AGLC; and

x. external (public) interfaces and the internal network must be tested.

6.1.3 **Cryptographic Controls –** Cryptographic controls must be implemented for the protection of information, in the following manner:

a) Any sensitive or personally identifiable information must be encrypted if sent over a network with a lower level of trust;

b) data that is not required to be hidden must be authenticated and 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 must 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 possible. If no such changes are available, the algorithm must be replaced;

g) encryption keys must not be stored without being encrypted themselves through a different encryption method and/or by using a different encryption key; and

h) must be used when the need to protect the confidentiality, authenticity, or integrity of the information being stored exists.

6.1.4 **Bi-Directional Requirements –** Significant emphasis must be placed on the integrity of the communication system for bi-directional data. Any system used to sell raffle ticket(s) through the Internet must 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.

6.1.5 **Connectivity –** Only authorized devices may be permitted to establish communications between any system components. The ERS must 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 is un-enrolled and disabled.

6.2 – Loss of Raffle Sales Unit Communications

6.2.1 **Loss of Communications –** A loss of communication between the RSU and the ERS must not affect the integrity of the critical memory.

6.2.2 **Continuing Sales -** An RSU 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 must be stored or cached on the RSU. The RSU must disable sales upon detecting the limit.

6.2.3 **Buffer and Cache Limits –** Reasonable buffer and cache limits must be established to permit the ERS to accommodate the load upon re-establishment of communication.

6.2.4 **Re-establishment of Communications –** Once communication is re-established, the system must require that the RSU re-authenticates with the ERS and transmits, uploads, or otherwise transfers all sales transactions completed during the communication loss.

6.2.5 **Secondary Communication –** 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.

6.3 – Electronic Raffle System Security

6.3.1 **General –** All communications, for ERSs with Internet connectivity, must pass through at least one approved application-level firewall and must not permit an alternate network path. Any alternate network path existing for redundancy purposes must also pass through at least one application-level firewall.

6.3.2 **Firewalls –** Firewalls must:

a) be located at the boundary of any two dissimilar security domains;

b) ensure all connections to the server used for the sale of tickets through the Internet must be housed in a secure data center and must pass through at least one application-level firewall. This includes connections to and from any non-related hosts used by the operator;

c) be a separate hardware device with the following characteristics:

   i. only firewall-related applications may reside on the firewall; and

   ii. only a limited number of accounts may be present on the firewall (e.g. system administrators only).

d) reject all connections except those that have been specifically approved;

e) reject all connections from destinations which cannot reside on the network from which the message originated;

f) disable all communication if the audit log becomes full.

6.3.3 **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 5.2 if the audit log is full. The audit log must contain:

a) all changes to configuration of the firewall;

b) reference clock for reporting; and

c) the source and destination IP address, Port Numbers, and MAC addresses.

6.3.4 **Remote Access –** Remote access refers to any access from outside the system or system network including any access from other networks within the same establishment.

Remote access may be permitted only if authorized by the AGLC. If remote access is permitted, it must accept only the remote connections permissible by the firewall application and ERS settings. If an ERS is using an RNG, the ERS must immediately detect remote access. The ERS must not permit the following functionality to a remote user:

a) unauthorized user administration functionality, including adding users or changing users;

b) access to any database other than information retrieval using existing functions; and

c) access to the operating system.

6.3.5 **Remote Access During a Raffle –** If remote access has been authorized, the ERS must:

a) disable remote access during the period of an active raffle; and

b) receive a temporary password from the local on-site administrator.

6.3.6 **Remote Access Auditing –** The ERS must maintain an activity log which updates automatically depicting all remote access information, to include:

a) verification that the system is operated by an authorized user. This may be done through documenting the 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.

6.3.7 **Third Party Hosting -** In cases where one or more component of the ERS is hosted by a third party service provider, the following requirements apply:

a) the private and financial information of all purchasers must be protected by the third party service provider using industry-standard ISS controls; and

b) third party services may not be used if they require software that is not in compliance with this ERSD.

6.3.8 **Wide Area Network (WAN) Communications** – WAN communications are permitted as approved by the AGLC and must meet the following requirements:

a) the communications over the WAN are secured from intrusion, interference, and eavesdropping; and

b) only functions documented in the communications protocol are permitted to be used over the WAN. The protocol specifications for the WAN must be provided by the ATF.

6.3.9 **Wireless Network Communications –** If a wireless communication solution is used, its use must be approved by the AGLC.

Section 7: Random Number Generator

7.1 – Random Number Generator (RNG) Requirements

7.1.1 **General –** The selection process for the winning number must be random and accomplished through the use of an approved RNG.

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

7.1.3 **RNG Entries** – Each valid, sold raffle ticket number must be available for random selection at the initiation of each drawing.

7.1.4 **Associated Equipment –** An electronic raffle system must use appropriate protocols to protect the RNG and random selection process from influence by associated equipment, which may be communicating with the ERS.

7.1.5 **RNG Integrity –** The RNG and random selection process must be impervious to influences from outside the ERS; including electro-magnetic interference, electro-static interference, and radio frequency interference. The use of an RNG must result in a selection that is:

a) unpredictable;
b) statistically independent;
c) conformed to the desired distribution; and
d) passable if evaluated against recognized statistical tests.

7.1.6 **RNG Software –** Software RNGs must demonstrate the following qualities:

a) the output of the RNG must be unpredictable. It must be computationally impossible to predict the next number without complete knowledge of the algorithm and seed value;
b) random number generation does not reproduce the same output stream, and two instances of an RNG must not produce the same output stream;
c) any forms of initialization, seeding, and re-seeding do not introduce predictability; and
d) seeding sources must be demonstrably random sources of entropy.

7.1.7 **RNG Testing –** The ATF will employ the use of various tests to determine whether or not the random values produced by the RNG pass the 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 (patters of occurrences must not be recurrent);

l) Interplay correlation test;

m) Serial correlation test potency and degree of serial correlation (outcomes must be independent of the previous games);

n) Tests of subsequences; and

o) Poisson distribution.

7.1.8 **RNG Audit-** The ERS must be capable of generating server data and electronic reports/records about the RNG ticket draw, for external storage from the server on durable electronic media.

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

7.1.10 **Background RNG Cycling/Activity Requirement –** In order to ensure that RNG outcomes cannot be predicted, adequate background cycling or activity must be implemented between each drawing at a speed that cannot be timed. The rate of background cycling or activity must be sufficiently random in and of itself to prevent prediction. The ATF must recognize that at some times during the raffle, the RNG may not be cycled when interrupts may be suspended. This is permitted, and must be kept to a minimum.

7.1.11 **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 must be randomly determined by an uncontrolled event. After every bearer ticket draw, there must be a random change in the RNG process (such as a new seed, a random timer, or a delay). This will verify the RNG and doesn’t start at the same value, every time. Random seeds may be used; 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 or 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.

7.1.12 **Scaling Algorithms –** the methods of scaling (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 is to be designed in such a way that all numbers within the lower range are equally probable.

b) If a particular random number that was 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.

7.1.13 **Winning Number Draw –** An ERS must use appropriate protocols to protect the RNG and random selection process from influence by associated equipment, which may be communicating with the electronic raffle system.