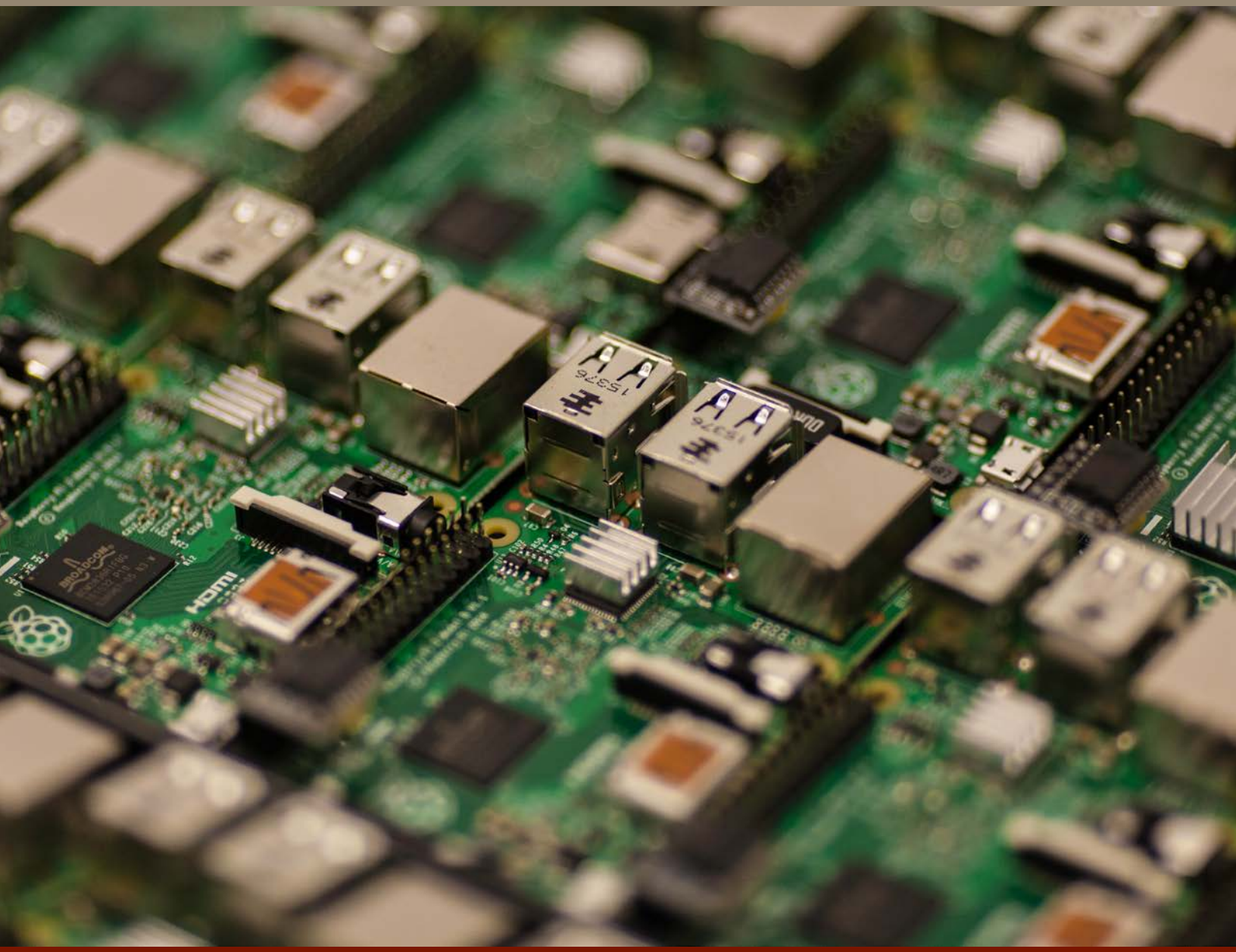
AGCO | Alcohol and Gaming Commission of Ontario

Ontario



ELECTRONIC RAFFLE SYSTEMS MINIMUM TECHNICAL STANDARDS

VERSION 1.0 NOVEMBER 2018

AGCO | Alcohol and Gaming Commission of Ontario

Alcohol and Gaming Commission of Ontario

90 SHEPPARD AVE E - SUITE 200
TORONTO ON M2N 0A4
Fax: 416 326-8711
Tel: 416 326-8700 or 1 800 522-2876 toll free in Ontario
www.agco.ca

Table of Contents

Introduction

The Registrar of Alcohol, Gaming and Racing is appointed under the Alcohol and Gaming Regulation and Public Protection Act, 1996 and has powers and duties under the Gaming Control Act, 1992 and its Regulations. Under section 3.8 of the Gaming Control Act, 1992, the Registrar is authorized to establish standards and requirements for the conduct, management and operation of Gaming Sites, lottery schemes or businesses related to a Gaming Site or a lottery scheme or for goods or services related to that conduct, management or operation. The Registrar has established these technical standards as the minimum standards for Electronic Raffle Systems (ERS) to comply with, in regards to their technical integrity, security, accounting capability, and the public interest.

These minimum Electronic Raffle standards are based on vulnerability-risk analysis of Raffle solutions, and reviewing other jurisdictional standards. The standards reflect typical ERS architecture, Raffle Game design and processes to mitigate inherent risks with technical integrity, security, accounting capability, and the public interest. The intent of this document is to provide minimum technical standards to be used in assessing the compliance of Electronic Raffle Systems for approval in Ontario, as applicable to a specific ERS technical solution for electronic Raffles.

These revised minimum technical standards are effective on November 30, 2018.

From time to time, as necessary, modifications will be made to these minimum technical standards.

Operational Requirements

These standards should be read in conjunction with Electronic Raffle Operational Terms and Conditions.

Introduction of New Technology in Ontario

The Alcohol and Gaming Commission of Ontario (AGCO) is a modern regulator, committed to ensuring that gaming is carried out in the Province of Ontario in keeping with the principles of technical integrity, security, accounting capability, and the public interest.

Recognizing that the gaming sector continues to evolve and that the introduction of new technologies provides opportunities for regulated entities in Ontario, the AGCO affirms its desire to address new technologies affecting the gaming sector in an efficient and open manner.

Therefore, where a Supplier or Charity has questions about the application of these standards to new technologies that seem to fall entirely or in part outside of the standards, the AGCO is open to engaging with Suppliers or Charities to understand the nature of those technologies and how and whether those technologies can be addressed by existing standards, either through their application or through the principles of technical integrity, security, accounting capability, and the public interest.

Submission Requirements

Suppliers must provide necessary information, training, and tools pertaining to the Electronic Raffle Systems that approval is being requested for to ensure the AGCO will be able to assess, test, and issue approval decisions without delay.

All requests for approval of Electronic Raffle Systems must adhere to the submission requirements, "AGCO Electronic Raffle Systems Submission Requirements", including being accompanied with fully and accurately completed AGCO submission form(s). This may be most efficiently achieved by Suppliers providing their submissions electronically to the AGCO in a secure fashion, e.g. via sFTP.

Glossary

- **AGCO** means the Alcohol and Gaming Commission of Ontario.
- **Associated Equipment:** Any equipment that is not part of Raffle Sales Unit (RSU) and is required for its complete operation, e.g. Raffle Prize display, printer and Backend System.
- **Cancelled Ticket:** A Raffle Ticket whose sale was cancelled.
- **Charity:** An organization that has met the eligibility criteria to hold a lottery licence under which it may conduct and manage a Raffle.
- **Backend System (also known as server)**: A dedicated computer system that is used to conduct and manage Raffle Games. It includes servers and databases.
- **Client Application**: Means any software downloaded or installed on a Raffle Sales Unit (RSU), or on off-the-shelf devices, such as PC//Mobile/Tablet devices that is used to facilitate Raffle sales via dedicated network, the internet and/or mobile public network
- **Critical Game Data:** Stored data that is vital to the conduct of Raffle. This includes, but is not limited to:
  a. Raffle sales (Ticket transactions including financial data);
  b. Raffle Numbers including selected winner(s);
  c. Prize distribution;
  d. POS/Ticket configurations;
  e. RSU Significant Events related to integrity, security and accounting; and
  f. Critical Game Software state (the last normal state before interruption)
- **Critical Game Software:** Any software that affects the integrity or outcome of the Raffle. This includes, but is not limited to, any software that is used to control Raffle functions, Raffle outcome, payout, security or accounting functions.
- **Critical Memory:** Memory locations storing Critical Game Data.
- **Discounted Ticket(s) (also known as Ticket price points)**: Raffle Ticket(s) with a specific number of Raffle Numbers sold at a discounted price, e.g. 3 for $5, 10 for $10, or 40 for $20.
- **Draw:** A random selection of winning Raffle Number(s) (or winners) conducted at a predetermined and scheduled time by means of a Random Number Generator.
- **Electronic Raffle System (ERS):** Includes hardware, software and applications for the purpose of conducting Raffles that:

a. Could influence the outcome of a Game held at a Gaming Site; or

b. Is integral to the conduct, management or operation of a Game.

- **Game:** A lottery scheme with the outcome based on Chance or mixed Chance and skill.
- **Gaming Site:** A premises or an electronic channel maintained for the purpose of playing or operating a lottery scheme.in the conduct, management or operation of lottery scheme.
- **Online:** Means using the internet to facilitate Raffle sales.
- **Point of Sale (POS):** Means hardware and/or software interface with Backend System that facilitates Raffle Ticket sales, e.g. RSU with its Client Application or Self-Service Application.
- **Prize:** A payout associated with winning Raffle Number(s).
- **Progressive Raffles or Progressive:** A Type of Raffle that increments the Prize based on the percentage of Raffle sales, or progresses another element of the Game until a certain condition is met to trigger and award the Progressive Prize.
- **Raffle:** A Game where Raffle Tickets are sold for a Chance to win a Prize at a Draw.
- **Raffle Number:** Unique ERS-generated number assigned to Raffle Ticket for the purpose of participating in Raffle Draw.
- **Raffle Ticket or Ticket:** Paper Ticket or an electronic record with Raffle Numbers, POS and Draw information, and may depending on type of Raffle contain player contact information.
- **Raffle Sales Unit (RSU):** Fixed base or mobile device, which communicates with Backend System to facilitate the sale of Raffle Tickets.
- **Randomness or Chance:** Observed unpredictability and absence of a pattern in a set of events that have definite probabilities of occurrence.
- **Random Number Generator (RNG):** Hardware and/or software used to generate numbers which exhibit Randomness.
- **Self-Service Application:** Means internet portal or Client Application on off-the-shelf devices, such as PC//Mobile/Tablet devices used to facilitate Raffle sale via the internet and/or mobile public network.
- **Significant Events:** Occurrences related to integrity, security and accounting including, but not limited to:

  a. Regular operation: Ticket transactions;

a. Irregular operation: errors in Ticket creation; and

b. Software authentication failure.

- **Software Storage Media (SSM):** Memory device used to store Critical Game Software, such as EPROMs, Compact Flash, Hard Drives, CD ROMs and DVDs.
- **Supplier**: Includes a Gaming Related Supplier and Non-Gaming-Related Supplier as set out in Regulation 78/12.
- **Validation Number**: A unique number which identifies Raffle Ticket that is used to validate the winning Raffle Number before Prize claim.
- **Voided Ticket**: A sold Raffle Ticket whose Raffle Numbers are removed from the pool of valid Raffle Numbers in ERS.

Part A: Point of Sale (POS)

1 RAFFLE SALES UNIT – RSU

1.1 GENERAL CONSTRUCTION

1.1.1 RSU must be secured to prevent unauthorized access to stored Critical Game Data and Critical Game Software.

1.1.2 Both mobile and fixed base RSU must resist tampering.

1.2 SECURITY AND INTEGRITY

1.2.1 Access to RSU Critical Game Software, Data, and configuration may only be possible via secure login.

1.2.2 Critical Game Software and Data including financial transaction data and gaming interaction information must be protected from alteration or corruption.

1.2.3 There must be a mechanism to retrieve Raffle sales data that has not been transmitted to the Backend System in the event of RSU failure.

1.3 COMMUNICATION WITH THE BACKEND SYSTEM

1.3.1 Significant Events must be communicated from RSU to the Backend System in real time or as soon as it becomes technically possible, e.g. when wireless communication is reestablished.

1.3.2 Interruptions in communication must not impact RSU integrity or security, e.g. any critical information related to Ticket transactions, and security events must be preserved.

1.4 ERROR CONDITIONS

1.4.1 RSU must be capable of immediately detecting, displaying and recording in error log error conditions that could affect its integrity, such as:

a) Critical Game Software errors:

i) defective Software Storage Media,

ii) authentication failure,

iii) communication errors, e.g. loss of communication with the Backend System;

b) Buffer full; and

c) Ticket printer failure.

1.4.2 Immediately upon an error condition from 1.4.1 being detected, impacted RSU functions must be disabled and may only be enabled after the condition has been resolved. In addition, the RSU must accurately communicate at a minimum the conditions set out in 1.4.1 a) and b) to the Backend System, whenever it is technically possible (e.g. within wireless range).

1.4.3 The integrity of Critical Game Data stored in Critical Memory must be maintained by methodology that enables failure detection, backup and recovery of Critical Game Data.

1.5 TICKET PRINTING

1.5.1 Complete and accurate Raffle information must be clearly presented on the Ticket.

1.5.2 In case of RSU shutdown by the Backend System, the current Ticket must be printed or Cancelled/Voided, and the RSU must display an explanatory message.

2 POS APPLICATIONS

2.1.1 The POS applications must display the name and version for the purpose of their verification.

2.1.2 Raffle sales must be communicated securely, completely and accurately between POS and Backend System.

2.1.3 The POS applications must provide sufficient information and messaging to sellers and players to facilitate raffle sales, e.g. when Raffle sale limits are reached, there must be proper messaging to sellers and players.

3 RAFFLE PRIZE DISPLAY

3.1.1 Raffle Prize displays must accurately show the Raffle Prize, which is clear to the player.

3.1.2 Upon verification, Raffle Draw results (the winning Raffle Number and final Raffle Prize) must be displayed accurately on all Raffle Prize displays.

Part B: Raffle Game

4 RAFFLE GAME DESIGN

4.1 GENERAL REQUIREMENTS

4.1.1 The ERS must ensure the integrity, security and accounting capability of all aspects of the Raffle, including but not limited to:

a) Sales (ordering, collection of player's data, if applicable, and payment process, assignment to Draw(s), issuance and cancellations/voiding of Raffle Tickets);

b) Selection of winner(s); and

c) Distribution of Prize(s).

4.1.2 Game designs and features must be clear and must not mislead the player.

4.2 RULES OF PLAY

4.2.1 Meaningful and accurate information must be provided to enable individuals to make informed choices.

At a minimum:

a) Meaningful and accurate information on the rules of play must be clearly stated and made available to players; and

b) Meaningful and accurate information on the odds of winning, payout odds or returns to players must be clearly stated and made available to players.

4.3 RAFFLE TICKET

4.3.1 Raffle Tickets must display the following information, at a minimum:

a) POS identifier;

b) Raffle Number(s);

c) Draw identifier; and

d) Draw date(s).

4.3.2 ERS must not generate duplicate Tickets for the same Draw. If reprint is featured, such a Ticket must be clearly marked as "reprint".

4.3.3 Raffle Numbers must be unique (no duplicates).

4.3.4 Ticket Validation Number, when implemented must be unique (no duplicates).

4.3.5 The price of Discounted Tickets must be clearly communicated to players.

4.4 PROGRESSIVE RAFFLES

4.4.1 All players participating in Progressive Raffles must be provided with the current contribution toward the Progressive Prize and any Progressive Prize amounts transferred to the next Draw.

4.4.2 Progressive Prize must be attainable for any of participating players, unless clearly stated otherwise in rules of play.

4.4.3 The following Progressive Raffles audit must be possible, at a minimum:

a) The configuration of Progressive Raffle;

b) The changes in the amount of Progressive Prize pot;

c) Draw ID, time and date of progressive hit; and

d) Progressive Prize awarded.

5 RAFFLE GAME PROCESSES

5.1 SALE OF RAFFLE TICKETS

5.1.1 Raffle Game may be provided only within Ontario.

5.1.2 Only eligible individuals are permitted to purchase Raffle Tickets. An individual under 18 years of age must not be permitted to play.

5.1.3 There must be clear confirmation that the purchase has been accepted and completed by the ERS.

5.1.4 The ERS must support cancellation of Ticket sale and voiding of sold Tickets prior to the close of the Raffle sales.

5.1.5 Cancelled and Voided Tickets must be logged, fully auditable, and any completed payments must be refunded to the player.

5.1.6 Voiding Raffle Tickets and cancelling Raffle purchases may only be performed by authorized personnel and must be fully auditable.

5.1.7 Raffle Numbers and corresponding Ticket Validation Numbers from Voided Tickets must not be possible to reissue or sell again for current Raffle Draw.

5.1.8 When ecommerce payment is integrated into the ERS, the payment processor and ERS must be compliant with current Payment Card Industry's Data Security Standards (PCI DSS).

5.2 ONLINE SALE

5.2.1 ERS must support secure player registration and player account creation, if implemented.

5.2.2 Relevant player information to uniquely identify a player for the purpose of Raffle sales, distribution and audit of Prizes must be collected and saved at the time of player registration, and must be verified to be complete and accurate before a player account is created.

Requirements – At a minimum, the following information must be gathered:

a) Full name;

b) Age information sufficient to confirm eligibility to play;

c) Address;

d) Method of identification for subsequent log on; and

e) Player contact information, e.g. phone number and email.

5.2.3 Before a player account is created, players must affirm that all player information provided upon registration is complete and accurate, and accept Raffle terms and conditions.

5.2.4 Only eligible individuals are permitted to create a player account and log on to their account.

5.2.5 Prior to purchasing Raffle Ticket, players must affirm that they are fit for play.

5.2.6 All player accounts must be uniquely identifiable.

5.2.7 Players may have only one player account with a Charity.

5.2.8 Player account information and Ticket transactions must be made readily available and clear to the player.

5.2.9 ERS supporting Online sales must provide full audit trail of events related to player account and Ticket transactions.

5.3 RSU SALE

5.3.1 RSU may sell Tickets when not communicating with the Backend System. During such time, all Ticket transactions must be buffered on the RSU, and upon the re-establishment of communication they must be transmitted to the Backend System.

5.3.2 The RSU functions that handle Raffle Tickets must perform as intended.

5.3.3 Improper activation of various RSU inputs and outputs must not compromise the integrity of Raffle.

5.4 RAFFLE DRAW(S)

5.4.1 Raffle Numbers Draw may only be conducted after:

a) Closure of the Raffle sales for the Draw;

b) Full reconciliation of all sold Tickets;

c) Full financial reconciliation of Tickets eligible for Draw;

d) Full financial reconciliation of sales, if necessary to determine Prize amount of the Draw; and

e) Verification that only valid Raffle Numbers are entered into the Draw.

5.4.2 The Raffle Draw must be conducted through a random selection process.

5.4.3 The Draw must include all sold valid Raffle Numbers, and exclude all invalid Raffle Numbers, e.g. unsold Tickets, Voided Tickets and Raffle Numbers from Cancelled Tickets that are not returned to the pool.

5.4.4 A winning Raffle Number must be drawn for each advertised Prize.

5.4.5 Backend System must accurately and securely log information related to each Raffle Draw.

5.5 VERIFICATION OF DRAW

5.5.1 The ERS must provide the ability to independently verify the results of each Raffle Draw if the outcome and recording of winning Tickets is not a fully automated process.

At a minimum, the following must be independently reconciled for each Draw prior to distributing the Prizes:

a) Selection of winners; and

b) Assignment of Prizes.

5.6 DISTRIBUTION OF PRIZE

5.6.1 Outcomes of the Raffles, as provided to players must be accurate, clear and easy to understand.

5.6.2 The Prize(s) must be awarded according to the advertised rules of play.

5.6.3 Winners must be notified in accordance with the approved rules of play.

5.6.4 Prizes must be distributed to the holder of the winning Tickets.

Part C: Electronic Raffle System (ERS)

6 SERVERS AND APPLICATIONS

6.1 DESIGN

6.1.1 All ERS components critical to the outcome of the Raffle must reside in Ontario.

6.1.2 Industry accepted components, both hardware and software, must be used where possible.

6.1.3 The ERS architecture must limit the loss of critical and sensitive data and Draw information.

6.1.4 A mechanism must be in place to ensure the reliability, integrity and availability of the ERS.

6.1.5 If other non-Raffle software or devices are present, they must not affect the integrity or outcome of Raffle Game or the interpretation of Game play or Game outcome.

6.1.6 The ERS may only display the minimum information about itself to unauthorized users and during ERS malfunctions.

6.1.7 The ERS components must have a method of synchronizing clocks.

6.1.8 The ERS and all devices must validate inputs before inputs are processed. In particular, user input fields must be validated to prevent malicious inputs from being processed.

6.1.9 ERS architecture must be designed and tested to ensure the integrity of the ERS under anticipated load.

6.1.10 The ERS architecture and all its related components must be designed with multiple layers of security (security in depth).

6.1.11 Sensitive data at rest and in transit must be protected for integrity and unauthorized access or use at all times using industry good practices.

6.1.12 Production, testing and development ERSs shall be logically separated.

6.1.13 ERS components must be restricted from the internet access.

6.2 RECOVERY

6.2.1 The ERS must be recoverable so that there is no impact on the integrity of the Raffle or the ability to audit the Raffle.

6.2.2 Where the ERS is not recoverable, the rules of play must clearly define the Charity's policies in respect of treating the player fairly when resolving the player's transactions.

6.3 ACCESS CONTROL

6.3.1 Users must be granted minimal access to the ERS based on business need.

Requirements – At a minimum:

a) Access privileges must be clearly documented; and

b) All ERS accounts must be uniquely assigned to an individual.

6.3.2 Any changes to user access privileges must be logged by the ERS to track: user performing the change, nature of the change, and time of the change.

At a minimum, the following actions must be logged:

a) Account creation;

b) Account removal;

c) Disabling/suspension of an account;

d) Password change;

e) Change in role; and

f) Change in permissions.

6.3.3 A secure authenticator that meets industry good practices (e.g. password, fingerprint) must be used to identify a user and his or her account to ensure that only authorized individuals are permitted to access their ERS account.

Requirements – At a minimum:

a) The ERS must automatically lock out accounts should identification and authorization requirements not be met after a defined number of attempts;

b) Passwords must not be communicated in plain text; and

c) The ERS must not have hardcoded passwords.

6.3.4 Physical and logical access to the ERS must be fully auditable and all related events must be logged.

6.3.5 The ERS must restrict unauthorized access to sensitive database files/tables, such

as stored procedures and passwords, and prevent their unauthorized alterations without the use of approved system functions, unless the database is encrypted.

6.4 SECURE CONFIGURATION

6.4.1 Only authorized personnel may be permitted to configure the Raffle Game and Ticket information.

6.4.2 Any and all setting or changing of Raffle configurations must be logged sufficiently for audit purposes, including: user, date/time and details of the change.

6.4.3 The ERS must have ability to enable only approved production Raffle configurations e.g. single Ticket for multi-event Draw or single event Draw, and single Ticket for multiple Draws, purchase/ordering of Tickets and distribution of Prizes.

6.4.4 ERS, data, activity logs and all other related components must be protected from threats, vulnerabilities, attacks or breaches to ensure the integrity and security of the ERS.

Requirements – At a minimum:

a) All users must be authenticated;

b) All ERS components and connections between the ERS and any other system, whether internal or external third party, must be hardened in accordance with industry and technology good practices prior to going live and prior to any changes; and

c) The ERS must be protected against malware.

6.4.5 Management or configuration of the Backend System must be technically restricted from POS.

6.4.6 The ERS must not allow Raffle configuration change that would adversely affect the security or integrity of the Raffle or any gaming-related information, once the sale of Raffle Tickets has commenced.

6.4.7 The Backend System must have the ability to monitor and manage all RSUs and sellers.

Requirements – At a minimum:

a) RSU must have a unique identifier that is sufficient to allow for its monitoring and tracking;

b) Non-authorized RSUs are not allowed to connect to Backend System;

c) Only authorized sellers can sell Ticket for a Raffle Draw after login to assigned RSUs;

d) Sellers access (credentials) can be enabled and disabled on-demand;

e) RSUs can be enabled or disabled on-demand for sale of Tickets; and

f) By default all RSUs are disabled for sale of Tickets, except during the time when assigned for sale of Tickets for a Raffle Draw.

6.5 MONITORING AND INCIDENT RESPONSE

6.5.1 Security activities must be logged in an auditable manner and monitored.

Requirements – At a minimum:

a) Attempts to attack, breach or access to ERS components in an unauthorized manner;

b) Intrusion attempts must be actively detected and where possible prevented from causing disruption or outage of the ERS; and

c) There must be adequate logging to capture and monitor any attempts to attack, breach or access in an unauthorized manner any components of the ERS.

6.6 DATA GOVERNANCE

6.6.1 Appropriate, accurate and complete records of transaction and Raffle information must be kept and made available to the Registrar for the purposes of audits and resolving player disputes.

6.6.2 The Backend Systems must record and store complete player information. Ticket and financial transactions (e.g. cash floats & collections), and Draw accounting data for all valid and Voided Tickets, including at a minimum:

a) Name of Charity conducting Raffle event;

b) The Draw ID, date and time;

c) Date and time of Ticket issuance;

d) Ticket price(s);

e) List of Prize(s), as applicable;

f) Value of Prize seeds, if any;

g) Winning Raffle Number(s) and Prize value(s);

h) Financial information sufficient to reconcile Ticket sales, including payment method and price points of sold Tickets;

i) Player information, including name, address, age and contact information;

j) Individual Ticket information per section 4.3.1;

k) Ticket status;

l) Ticket transactions history, including Voided and Cancelled of Tickets;

m) Type of transaction or other method of differentiating ticket types; and

n) POS and User ID for individual Tickets.

6.6.3 Adjustments and corrections to Critical Game Data are permitted by authorized individuals, provided the following information is recorded in unalterable log:

a) Name of authorized user who performed the change;

b) Date and time of change;

c) Type of data changed; and

d) The value of data before and after change.

6.6.4 Data governance must preserve data processing integrity and protect sensitive data.

6.6.5 Sensitive data, including player information, financial transactions, credit/debit card information and data relevant to determining Raffle outcomes, must be secured and protected from unauthorized access or use at all times.

Requirements – At a minimum:

a) The ERS must ensure that data is appropriately backed up in a manner that allows it to be completely and accurately restored.

6.7 LOGGING AND REPORTING

6.7.1 The ERS must at a minimum contain the following information in reports for complete audit trail, capable of being generated on-demand, for settable time periods, and for specific activities:

a) Raffle Transactions - Information on all Ticket transactions and Draw accounting handled by the ERS, including: all valid, Cancelled and Voided Tickets with Raffle Numbers and Validation Numbers, Ticket price, transaction POS identifier, time of transaction, Prize seed(s), total sales, cash floats & collections, winning Raffle Numbers and Prizes distributed;

b) Security Events – any information on access and attempted authentication including: component accessed, username, success or failure of authentication, time, any changes made; and

c) Error Logs – All critical errors, e.g. failed software authentication and communication errors.

7 RANDOMNESS OF RAFFLE DRAWS

7.1 SOFTWARE RANDOM NUMBER GENERATOR (RNG)

The following requirements are applicable to software Random Number Generators and their implementation.

7.1.1 Random numbers must be:

a) Statistically independent;

b) All values within the desired range must have an equal Chance of being generated;

c) Able to pass various recognized statistical tests; and

d) Unpredictable.

7.1.2 The range of random numbers must correspond to the range used in a particular Game including both high and low end of Raffle sales. Specifically, the random numbers must produce statistics that lie within the 99% confidence interval for various Game specific, empirical statistical tests, including but not limited to frequency test, runs test and serial correlation test.

7.1.3 The RNG output must not exhibit detectable patterns or correlation with any previous RNG output.

7.1.4 The ERS must not make any secondary decision to change the winning Raffle numbers.

7.1.5 Where the Draw process of winning Raffle Numbers is interrupted, the original selection must be preserved until full ERS recovery.

7.1.6 The ERS must use secure communication protocols to protect RNG and random selection process.

7.1.7 Pools of Raffle Numbers must be stored securely.

7.2 PHYSICAL RANDOMIZERS

7.2.1 If applicable, physical randomizers that use the laws of physics to determine winning Raffle Ticket, must ensure Raffle Game integrity and Randomness of Raffle Draws (e.g. shuffling of Tickets).

Note: The Randomness and implementation of physical randomizers will be assessed on a case-by-case basis.

8 INTEGRITY OF CRITICAL GAME SOFTWARE

8.1 AUTHENTICATION OF CRITICAL GAME SOFTWARE

8.1.1 The ERS must be able to detect unauthorized changes.

8.1.2 A mechanism that meets industry good practices must be built into the ERS to verify the integrity of the Critical Game Software in production, to ensure the approved software is being used, no unauthorized changes and Raffles operate as intended.

At a minimum, ERS must be successfully authenticated:

a) Immediately prior to the startup of Raffle event;

b) Before Raffle Draw for jackpot Prizes; and

c) On demand by the Charity, or AGCO.

Note: The authentication method will be evaluated on a case-by-case basis and approved by the Registrar based on good industry practices. If the ERS does not have the capability to self-authenticate, the Charity may perform this authentication manually until self-authentication is available.

8.1.3 If the self-authentication fails, the software that fails authentication must enter an error condition, safely stop operation and notify the Charity. The AGCO and the Charity must be immediately notified of the failure, including the details of the failed authentication.

8.1.4 The results of each authentication must be recorded in an unalterable report which is available to the AGCO. This report must include a pass/fail condition with details on which software did not pass the authentication.

on which software did not pass the authentication.

8.2 VERIFICATION OF RSU CRITICAL GAME SOFTWARE BY BACKEND SYSTEM

8.2.1 Backend System must initiate independent verification on any client device or RSU Critical Game Software upon establishment of a connection with the system. When a threshold of unsuccessful verification attempts is reached, such client device or RSU must be disabled.

Note: An alternative method based on good industry practices that mitigates this risk may be evaluated on a case-by-case basis and approved by the Registrar.

OTHER TECHNICAL REQUIREMENTS

9 NETWORK INFRASTRUCTURE

9.1.1 Communication protocol among ERS components must meet the following minimum requirements:

a) Only documented functions may be used over network infrastructure; and

b) Each ERS component must function per the protocol.

9.1.2 System time requirements in 6.1.8 also apply to network equipment, to preserve logging and auditing capability.

9.1.3 All gaming related network traffic exposed to public network lines must be secured using an industry standard method proven to prevent any security threats.

9.1.4 Network architecture must be designed such that traffic is controlled to prevent a large volume of communications causing an integrity issue for players.

10 REMOTE ACCESS AND MONITORING

10.1.1 Any remote access methods and associated procedures must limit access to authorized users and systems to perform specific tasks only through a secure link.

10.1.2 Remote access to ERS may only be granted to either the Charity or the registered Supplier from their respective secure business network, such as VPN client with two-factor authentication, provided the ERS automatically monitors and records the log-on name, time and date the connection was made, duration of the connection, and activity while logged-in, including the specific areas accessed and Raffle related changes made.

11 INDEPENDENT SECURITY ASSESSMENT

11.1.1 New ERS that is publicly exposed (e.g. Web applications accessible through public networks) must be assessed in accordance with industry good practice security frameworks by qualified individuals to ensure that security vulnerabilities are identified and assessed, and risks are confirmed to be negligible through security/ penetration testing, as applicable.

11.1.2 Modifications to publicly exposed gaming applications may require assessment per 11.1.1 to be performed on the modifications, depending on the complexity and number of changes. These will be assessed on a case-by-case basis.