PUBLIC PROTECTION CABINET
Department of Charitable Gaming
(As Amended at ARRS, November 9, 2020)

820 KAR 1:050. Raffles.

RELATES TO: KRS 238.545, 238.550

STATUTORY AUTHORITY: KRS 238.515

NECESSITY, FUNCTION, AND CONFORMITY: KRS 238.515 authorizes the Department of Charitable Gaming to establish and enforce reasonable standards for the conduct of charitable gaming and to promulgate administrative regulations necessary to implement KRS Chapter 238. This administrative regulation establishes standards for the conduct of raffles.

Section 1. ***Definitions. (1) “Access control” means the restriction of access to a place or other resource. Locks and login credentials are two (2) mechanisms of access control.***

(2) “Address Resolution Protocol (ARP)” is the protocol used to translate IP addresses into MAC addresses to support communication on a LAN (Local Area Network). The Address Resolution Protocol is a request and reply protocol and it is communicated within the boundaries of a single network, never routed across internetwork nodes (connection points, either a redistribution point or an end point for data transmissions).

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

(4) “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.

(5) “Bearer ticket” means an electronic or paper ticket that contains one (1) or more draw numbers purchased.

(6) “Bi-Directional” means the ability to move, transfer, or transmit in both directions.

(7) “Counterfoil” means an electronic record or paper ticket stub, also known as a barrel ticket, which shall be drawn to determine a winner and contains a player's draw number matching the bearer ticket purchased and may, depending on the type of raffle, contain the name, address, or telephone number of the player.

(8) Critical memory means memory that is used to store all data that is considered vital to the continued operation of the RSU.

(9) “Crypto-analytic” means an attack against the encryption key (refer to definition of encryption key).

(10) “Cryptographic” means anything written in a secret code or cipher.

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

(12) “Domain” is a term used to identify one (1) or more IP addresses. A domain name is used in a Uniform Resource Locator (URL) to identify particular Web pages.

(13) “Draw number” means a uniquely identifiable number that is provided to the purchaser for each chance purchased and may be selected as the winning number for the raffle.

(14) “Electronic raffle system” means computer software and related equipment used by raffle licensees to sell tickets, account for sales, and facilitate the drawing of tickets to determine the winners.

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

(16) “Encryption key” means a sequence of numbers used to encrypt or decrypt (to decode/decipher) data.

(17) “Firewall” means any number of security schemes that prevent unauthorized users from gaining access to a computer network or that monitor transfers of information to and from the network.

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

(19) “Host” means a computer system that is accessed by a user working at a remote location. Typically, the term is used when there are two (2) computer systems connected by modems and telephone lines. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal. A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

(20) “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 shall take in response to various commands.

(21) “Internet” means an interconnected system of networks that connects computers around the world via the TCP/IP protocol. TCP/IP protocol is short for Transmission Control Protocol/Internet Protocol, the suite of communications protocols used to connect hosts on the Internet.

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

(23) “Internet Protocol (IP)” means an identifier for a computer or device on a TCP/IP network.

(24) “Media Access Control (MAC)” means a hardware address that uniquely identifies each node, such as the computer or printer, of a network.

(25) “Man-in-the-Middle (MITM)” means an active Internet attack where the person attacking attempts to intercept, read, or alter information moving between two (2) computers.

(26) “Message authentication” means a security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.

(27) “Online” means being connected to the Internet.

(28) “Online Purchasing Platform” means the raffle system hardware and software that drives the features common to all raffles offered, and which forms the primary interface to the Raffle System for both the patron and the operator. The online

purchasing platform provides the patron with the means to register an account, log in to or out of their account, modify their account information, make ticket purchases, request account activity statement or reports, and close their account. In addition, any web pages displayed to the patron that relate to ticket purchasing offered on the raffle system. The online purchasing platform provides the operator with the means to review patron accounts, enable or disable raffles, generate various financial transaction and account reports, input raffle outcomes, enable or disable patron accounts, and set any configurable parameters.

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

(30) "Raffle sales unit (RSU)" means a portable or wireless device, a remote hardwired connected device, or a standalone cashier station that is used as a point of sale for bearer tickets.

(31) "Remote access" means any access from outside the system or system network including any access from other networks within the same establishment.

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

(33) "Security certificate" means information, often stored as a text file, which is used by the Secure Socket Layers (SSL) protocol to establish a secure connection. A security certificate contains information about whom it belongs to, who it was issued by, valid dates, and a unique serial number or other unique identification that may be used to verify the contents of the certificate. In order for an SSL connection to be created, both sides are required to have a valid security certificate, which is also called a digital ID.

(34) "Stateful firewall" means a firewall that keeps track of the state of network connections traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection shall be allowed by the firewall; others shall be rejected. Stateful inspection, also referred to as Dynamic Packet Filtering, is a security feature often included in business networks,

(35) "Stateless" means a communications protocol 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. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. In contrast, a protocol that requires the keeping of internal state is known as a stateful protocol. Examples of stateless protocols include Internet Protocol (IP) and the Hypertext Transfer Protocol (HTTP).

(36) "Validation number" means a unique number that may represent one (1) or more draw numbers that shall be used to validate the winning number for the raffle.

Section 2. Raffle Ticket Construction. (1) Raffle tickets shall have a detachable section or duplicate ticket and shall be consecutively numbered. If raffle tickets are sold electronically, the charitable organization selling the tickets shall provide all purchasers with a physical ticket or electronic communication that contains the information required by subsection (2) ***of this section***.

(2) The detachable section or duplicate of the ticket shall bear a duplicate number corresponding to the number on the ticket and shall provide space for the purchaser's name, complete address, and telephone number.

(3) The following information shall be on each ticket:

(a) The date and time for each drawing;

(b) The location of each drawing;

(c) The name of the charitable organization conducting the raffle;

(d) The charitable organization's license number or exemption number;

(e) The price of the ticket; and

(f) Each prize to be awarded with a fair market value over $500.

(4) The requirements of subsections (2) and (3) of this section shall be waived if:

(a) The raffle tickets sell for five (5) dollars or less, or

(b) The raffle sales are initiated and concluded and all winners are selected at a licensed charity fundraising event or a licensed special limited charity fundraising event.

Section ***(3)[~~2.~~]*** Raffle Prizes. (1) A charitable organization conducting a raffle in which real or personal property prizes are to be awarded shall be responsible for the transfer and delivery of the prize without lien or interest of others.

(2) All raffle prizes shall be awarded as indicated on the raffle ticket unless the event at which the raffle was to be conducted is postponed. If the raffle is postponed, all reasonable efforts shall be made to notify ticket holders of the new drawing date.

(3) If the prize to be awarded is the jackpot of a progressive raffle board, the charitable organization's charitable gaming session records shall report in the gross receipts total all startup cash, monies derived from raffle ticket sales, and any other contribution to the jackpot.

Section ***(4)[~~3.~~]*** Conduct of Raffles. (1) Any person holding a raffle ticket shall be permitted to observe the raffle drawing. **A charitable organization may broadcast a raffle drawing via a verifiable online live streaming service to provide ticket holders an opportunity to view the drawing if the charitable organization provides purchasers *with* instructions for viewing the drawing at the time tickets are purchased.**

(2) A person shall not be required to be present at a raffle drawing in order to be eligible for the prize drawing.

(3) For raffles using paper tickets, each [~~Each~~] ticket seller shall return to the charitable organization the stubs or other detachable sections or duplicates of all tickets sold prior to the drawing.

(4) For raffles using paper tickets, before [~~Before~~] drawing, the charitable organization shall place the seller's portion of each ticket sold into a receptacle from which the winning tickets are to be drawn. The receptacle shall be designed so that each ticket placed in it has an equal chance to be drawn.

(5) If a charitable organization uses electronic raffle software to conduct a raffle, the charitable organization shall ensure that the electronic raffle software has been:

(a) Purchased, leased, or otherwise obtained from a distributor licensed by the department;

(b) Manufactured by a manufacturer licensed by the department;

(c) Certified by an independent testing lab; and

(d) Approved by the department for use in the Commonwealth.

(6) A charitable organization shall conduct a raffle entirely with **traditional** paper tickets or entirely with **an** electronic **or online raffle system [~~tickets~~]**; a charitable organization shall not use both paper and electronic tickets in the same raffle**, except for paper receipts or bearer tickets generated by an electronic or online raffle system in compliance with this regulation**.

Section ***(5)[~~4.~~]*** Claiming Raffle Prizes. (1) If the winner is not present at the drawing, the charitable organization shall notify the winner within seven (7) days of the drawing that the winner shall claim the prize within thirty (30) days.

(2) If a winner does not wish to claim the prize but wishes to donate it to the charitable organization, the charitable organization shall obtain a written statement of the winner’s intention within the thirty (30) day period. A charitable organization shall not accept the donation to the charitable organization of a prize won if doing so would violate KRS 238.540.

(3) If a raffle winner does not claim the prize or donate it to the charitable organization within thirty (30) days after having been contacted by certified mail, or if the raffle winner is ineligible by law to claim the prize, the charitable organization shall notify the department and draw another ticket in the presence of department personnel.

(4) The requirements of subsections (1), (2), and (3) of this section shall be waived, and the charitable organization shall be allowed to draw tickets until a winner is present if:

(a) The raffle tickets sell for five (5) dollars or less;

(b) The raffle sales are initiated and concluded and all winners are selected at a licensed charity fundraising event; or

(c) The raffle sales are initiated and concluded and all winners are selected at a licensed special limited charity fundraising event.

[~~Section 5. Electronic Raffle Definitions. (1) “Bearer ticket” means an electronic or paper ticket that contains one or more draw numbers purchased.~~

~~(2) “Counterfoil” means an electronic record or paper ticket stub, also known as a barrel ticket, which will be drawn to determine a winner and contains a single draw number matching the player's purchased bearer ticket and may, depending on the type of raffle, contain the name, address, or telephone number of the player.~~

~~(3) “Draw number” means a uniquely identifiable number that is provided to the purchaser for each chance purchased and may be selected as the winning number for the raffle.~~

~~(4) “Electronic raffle system” means computer software and related equipment used by raffle licensees to sell tickets, account for sales, and facilitate the drawing of tickets to determine the winners.~~

~~(5) “Raffle sales unit” (or “RSU”) means a portable and/or wireless device, a remote hardwired connected device or a standalone cashier station that is used as a point of sale for bearer tickets.~~

~~(6) “Validation number” means a unique number which may represent one or more draw numbers that will be used to validate the winning number for the raffle.~~]

Section 6. Electronic Raffle System Standards. (1) Each electronic raffle system shall have a device or facility that provides for the sale of bearer tickets and the collection and accounting tools needed to track all sales initiated through the raffle system. The system shall have the ability to support all RSUs, whether they are hard-wired or connected wirelessly, to ensure that each RSU sends or transmits all ticket sales to the system. The system shall have the ability to facilitate winner selection by either manual or electronic means.

(2) Time Limits***.[~~:~~]*** The electronic raffle system software ***shall [~~must~~]*** be capable of setting time limits for when tickets may be purchased for a raffle drawing.

(3) Configuration Changes***.[~~:~~]*** After the commencement of a raffle, the electronic raffle system software shall not allow changes to parameters ***that [~~which~~]*** may affect the integrity of the raffle.

(4) Bearer Tickets***.[~~:~~]*** After the payment of a fee, participants shall receive a bearer ticket for one ***(1)*** or more chances to win a raffle drawing. The bearer ticket shall be printed with the information required by Section ***(2)[~~1~~]***(2) of this administrative regulation ***and shall include[~~and~~]***:

(a) The date and time (in twenty-four (24) hour format showing hours and minutes) that the ticket was purchased;

(b) All unique draw numbers purchased for the raffle;

(c) The RSU identifier from which the ticket was generated; and

(d) A unique validation number or barcode.

(5) Validation Numbers***.[~~:~~]*** The algorithm or method used by the electronic raffle system to generate the bearer ticket validation number ***shall [~~must~~]*** be unpredictable and ensure against duplicate validation numbers for the raffle currently in progress.

(6) Voiding a Ticket***.[~~:~~]*** The electronic raffle system shall be designed to flag or otherwise identify a voided bearer ticket and its corresponding draw number. The system shall record at a minimum the draw numbers and the validation number from the voided bearer ticket. Voided draw numbers shall not be able to be resold or reissued for that raffle.

(7) Counterfoils***.[~~:~~] If [~~Where~~]*** a manual draw is used to determine a winner, all counterfoils used in a raffle drawing ***shall [~~must~~]*** be the same size, shape, and weight. A counterfoil shall be printed or stored electronically for each purchased draw number. If an electronic random number generator is used to determine the winner of the raffle drawing, a printed counterfoil is not required. A counterfoil ***shall [~~must~~]*** only contain one ***(1)*** draw number and shall contain the following information, which matches the bearer ticket issued to the player:

(a) Event Identifier or Location;

(b) The draw number;

(c) Issued date and time (in twenty-four (24) hour format showing hours and minutes);

(d) Value or cost of the bearer ticket; and

(e) Unique validation number or barcode.

(8) Reprinting of Counterfoils***.[~~:~~] If [~~Where~~]*** the system supports the reprinting of counterfoil tickets, ***the [~~this~~]*** facility shall require additional supervised access controls, and the draw numbers for all reprinted counterfoils shall be flagged in the system as reprints.

(9) Raffle Prize Displays***.[~~:~~]*** An electronic raffle system may include a raffle prize display that ***may [~~can~~]*** be viewed by participants of the raffle that displays the raffle prize and the current progression of the prize. The electronic raffle system may have multiple raffle awards displayed in an alternating fashion.

(10) Electronic Raffle Drawing Requirements***.[~~:~~]*** A raffle drawing shall be held at a date, time, place stated on the charitable organization's license or certificate of exemption. The drawing shall be administered by an officer or chairperson of the charitable organization. A raffle drawing shall only be conducted after:

(a) The close of the raffle; and

(b) All sales and voided sales for the particular raffle purchase period have been reconciled.

(11) Closing the Raffle Purchase Period***.[~~:~~]*** The system ***shall [~~must~~]*** be capable of closing off the sale of bearer tickets at a time determined by the operator. ***Tickets shall not be sold [~~No sales of tickets may occur~~]*** after the raffle purchase period has ***[~~been~~]*** closed. The system ***shall [~~must~~]*** be capable of displaying to the operator by way of the RSU device display that all sales from a particular device have been uploaded, transferred***,*** or otherwise communicated to the electronic raffle system.

(a) On verification of the sales data transfer, the RSU device ***shall [~~must~~]*** be capable of being reset or closed; and

(b) The RSU ***shall [~~must~~]*** not be enabled for any further sales for the current raffle.

(12) Voided Tickets***.[~~:~~]***Voided tickets shall not be qualified toward any prize. The system shall be capable of reconciling voided sales for the raffle purchase to identify all voided tickets that may be committed to the draw. The system shall record an acknowledgement from the event manager that voided tickets have been reconciled before permitting a winning number to be entered into the system for validation.

(13) Winner Determination***.[~~:~~]*** The operator shall conduct an electronic or other approved draw procedure ***that [~~which~~]***ensures a randomly selected draw number as a winner from all tickets sold. Each drawn counterfoil shall be verified as a sold and valid ticket. This process shall be repeated for each advertised prize.

(14) Official Drawing Results***.[~~:~~]*** Results of the drawing become official and final after the drawn number is verified as a winning bearer ticket for the respective drawing, and is presented to the participants of the raffle. The system shall display the winning draw on all capable display devices ***[~~that are~~]*** intended to be viewed by participants.

(15) Winner Verification***.[~~:~~]*** Winning tickets shall be verified prior to payout. Participants ***shall [~~must~~]*** present the bearer ticket to an authorized agent for validation with the system. The system shall be capable of verifying the winning draw numbers and shall allow for the validation of draw numbers either manually or through the use of a bar code scanner or equivalent.

(16) System Reporting Requirements***.[~~:~~]*** The system shall be capable of producing general accounting reports to include the following information for each draw conducted:

(a) Raffle Drawing Report. A report ***that [~~which~~]*** includes the following for each raffle drawing:

1. Date and time of the event;
2. Organization running the event;
3. Sales information;
4. Prize value awarded to participant;
5. Prize distribution (total raffle sales vs. prize value awarded to participant)***;***
6. Refund totals by event;
7. Draw numbers-in-play count;
8. Winning number(s) drawn (including draw order, call time, and claim status); and
9. All other information required by 820 KAR 1:057.

(b) Exception Report***.[~~:~~]*** A report ***that [~~which~~]*** includes system exception information, including***[~~, but not limited to,~~]*** changes to system parameters, corrections, overrides, and voids;

(c) Bearer Tickets Report***.[~~:~~]***A report ***that [~~which~~]*** includes a list of all bearer tickets sold including all associated draw numbers, selling price, and RSU identifier;

(d) Sales by RSU***.[~~:~~]*** A report ***that [~~which~~]*** includes a breakdown of each RSU's total sales (including draw numbers sold) and any voided ***or [~~and~~]*** misprinted tickets;

(e) Voided Draw Number Report***.[~~:~~]*** A report ***that [~~which~~]*** includes a list of all draw numbers that have been voided including corresponding validation numbers;

(f) Raffle Sales Unit Event Log***.[~~:~~]*** A report ***that [~~which~~]*** lists all events recorded for each RSU, including the date and time and a brief text description of the event or identifying code***;[~~.~~]***

(g) Raffle Sales Unit Corruption Log***.[~~:~~]*** A report ***that [~~which~~]*** lists all RSUs unable to be reconciled to the system, including the RSU identifier, RSU operator, and the money collected; ***and***

(h) All information required by 820 KAR 1:057.

Section 7. Raffle Sales Unit Standards. (1) After the payment of a fee, participants shall receive a chance to win a raffle drawing. A chance to win a raffle drawing shall be purchased from an attendant-operated Raffle Sales Unit (***[~~“~~]***RSU***[~~”~~]***).

(a) 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 ***shall [~~will~~]*** provide the participant the bearer ticket(s) purchased by the participant.

(b) 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 for the ticket(s), the RSU ***shall [~~will~~]*** issue the corresponding bearer ticket(s) purchased by the participant.

(2) An RSU ***shall [~~must~~]*** be capable of generating and printing a bearer ticket with one ***(1)*** or more uniquely identifiable draw numbers.

(a) The system ***shall [~~must~~]*** not generate duplicate draw numbers within the same event.

(b) For each draw number generated, there ***shall [~~must~~]*** be ***only*** one ***(1) [~~and only one~~]*** corresponding counterfoil with the same draw number.

(c) The RSU ***shall [~~must~~]*** be capable of providing a transaction receipt in the form of a bearer ticket to a purchaser.

(3) Access Controls***.[~~:~~]***Access to raffle sales software shall be controlled by a secure logon procedure. It shall not be possible to modify the configuration settings of an RSU without an authorized secure logon.

(4) Touch Screens***.[~~:~~]*** Touch screens shall be accurate once calibrated and shall maintain that accuracy for at least the manufacturer's recommended maintenance period.

(5) RSU Interface***.[~~:~~]*** The functions of all buttons, touch or click points represented on the RSU interface shall be clearly indicated within the area of the button, ***[~~or~~]*** touch ***or[~~/~~]***click point ***[~~and/~~]***or within the help menu. There shall be no functionality available through any buttons or touch ***or[~~/~~]***click points on the RSU that are undocumented.

(6) Communications***.[~~:~~]*** A Raffle Sales Unit ***shall [~~must~~]*** be designed or programmed ***to [~~such that it may~~]*** only communicate with authorized electronic raffle systems components. The electronic raffle system ***shall [~~must~~]*** have the capability to uniquely identify and authorize each RSU used to sell tickets for a raffle.

(7) Wireless Raffle Sales Units***.[~~:~~]*** Communication ***shall [~~must~~]*** only occur between the RSU and the electronic raffle system via authorized access points.

(8) Printing Bearer Tickets***.[~~:~~]*** If the RSU connects to a printer that is used to produce bearer tickets, the bearer ticket shall include information as indicated in Section ***2 [~~1~~]***(2) ***of this administrative regulation***. ***This information, or some of this information, [~~It~~]*** may be ***[~~permissible for some of this information to be~~]*** contained on the ticket stock itself.

(a) The RSU ***shall [~~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.

(b) If a barcode forms part of the validation number printed on the bearer ticket, the printer ***shall [~~must~~]*** support the barcode format and print with sufficient resolution to permit validation by a barcode reader.

(9) Printer Error Conditions***.[~~:~~]***The bearer ticket printer shall be able to detect and indicate to the operator the following error conditions:

(a) Low battery;

(b) Out of paper or paper low;

(c) Printer disconnected ***([~~-~~]***It is permissible for the system to detect this error condition when it tries to print***)***.

(d) If the unit is capable of reprinting a ticket, the reprinted ticket shall clearly indicate that it is a reprint of the original ticket.

(10) Critical Memory Requirements***.[~~:~~] [~~Critical memory means memory that is used to store all data that is considered vital to the continued operation of the RSU.~~]*** Critical memory shall be maintained for the purpose of storing and preserving critical data ***including[~~. This includes, but is not limited to~~]***:

(a) ***If [~~When~~]*** not communicating with the system, recall of all tickets sold including, at minimum, draw numbers and validation numbers; and

(b) RSU configuration data.

(11) Maintenance of Critical Memory***.[~~:~~]*** Critical memory storage shall be maintained by a methodology that enables errors to be identified. This methodology may involve signatures, checksums, partial checksums, multiple copies, time stamps ***[~~and/~~]***or effective use of validity codes.

(12) Comprehensive Checks***.[~~:~~]*** Comprehensive checks of critical memory shall be made on startup and shall detect failures with an extremely high level of accuracy.

(13) Unrecoverable Critical Memory. An unrecoverable corruption of critical memory shall result in an error. Upon detection, the raffle sales unit shall cease to function.

(14) Backup Requirements. The RSU ***shall [~~must~~]*** have a backup or archive capability, which allows the recovery of critical data ***if [~~should~~]*** a failure occurs.

(15) RSU Program Identification***.[~~:~~]*** All programs shall 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.

(16) Detection of Program Corruption***.[~~:~~]*** RSU programs shall be capable of detecting program corruption and cause the RSU to cease operations until corrected.

(17) Verification of Program Updates***.[~~:~~]*** Prior to execution of the updated software, the software ***shall [~~must~~]*** be successfully authenticated on the RSU.

(18) Independent Control Program Verification***.[~~:~~]*** The RSU shall 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 ***shall [~~must~~]*** be accomplished by being authenticated by a third-party device or by allowing for removal of the media ***so [~~such~~]*** that it ***may [~~can~~]*** be verified externally. This integrity check ***shall [~~will~~]*** provide a means for field verification of the software to identify and validate the program. The test laboratory, prior to device approval, shall evaluate the integrity check method.

Section 8. Random Number Generator Requirements. (1) A random number generator shall reside on a program storage device secured in the logic board of the system. The numbers selected by the random number generator for each drawing shall be stored in the system's memory and be capable of being output to produce a winning number. The use of an RNG results in the selection of raffle outcomes in which the selection shall:

(a) Be statistically independent;

(b) Conform to the desired random distribution;

(c) Pass industry-standard recognized statistical tests, as chosen by the independent testing laboratory; and

(d) Be unpredictable.

(2) Applied Tests. The test laboratory may employ the use of various recognized tests to determine whether or not the random values produced by the random number generator pass the desired confidence level of ***ninety-nine (99) percent [***~~99%~~***]***. The independent test lab shall choose the appropriate tests on a case by case basis depending on the RNG under review. 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-Smimov test;
(i) Adjacency criterion tests;
(j) Order statistic test;
(k) Runs tests (patterns of occurrences ***shall [~~should~~]*** not be recurrent);
(l) Interplay correlation test;
(m) Serial correlation test potency and degree of serial correlation (outcomes ***shall [~~should~~]*** be independent of the previous game);
(n) Tests on subsequences; and
(o) Poisson distribution.

(3) Period***.[~~:~~]*** The period of the RNG, in conjunction with the methods of implementing the RNG outcomes, ***shall [~~must~~]***be sufficiently large to ensure that all valid, sold numbers are available for random selection.

(4) Range***.[~~:~~]*** The range of raw values produced by the RNG ***shall [~~must~~]*** be sufficiently large to provide adequate precision and flexibility when scaling and mapping.

(5) Background RNG Cycling or Activity Requirement***.[~~:~~] [~~In order~~]*** To ensure that RNG outcomes cannot be predicted, adequate background cycling or activity ***shall [~~must~~]*** be implemented between each drawing at a speed that cannot be timed. The rate of background cycling or activity ***shall [~~must~~]*** be sufficiently random in and of itself to prevent prediction.

(6) RNG Seeding or Re-Seeding***.[~~:~~]*** The methods of seeding or re-seeding implemented in the RNG ***shall [~~must~~]*** ensure that all seed values are determined securely and that the resultant sequence of outcomes is not predictable.

(a) The first seed shall be randomly determined by an uncontrolled event. After every bearer ticket draw, there shall be a random change in the RNG process (new seed, random timer, ***or*** delay, ***[~~etc.~~]***). This ***shall [~~will~~]*** verify the RNG does not start at the same value, every time. It is permissible not to use a random seed***, except[~~; however,~~]*** the manufacturer ***shall [~~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 ***shall [~~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 ***shall [~~must~~]*** be a function of the value produced by the RNG immediately prior to the interruption.

(7) Scaling Algorithms. The methods of scaling (***[~~i.e.~~]*** converting raw RNG outcomes of a greater range into scaled RNG outcomes of a lesser range) shall be linear, and shall not introduce any bias, pattern***,*** or predictability. The scaled RNG outcomes ***shall [~~must~~]*** be proven to pass various recognized statistical tests as chosen by the independent testing laboratory.

(a) If a random number with a range shorter than that provided by the RNG is required for some purpose within the raffle system, the method of re-scaling, (***[~~i.e.,~~]*** converting the number to the lower range), ***shall [~~is to~~]*** be designed in ***[~~such~~]*** a way that all numbers within the lower range are equally probable.

(b) If a particular random number selected is outside the range of equal distribution of rescaling values, it is permissible to discard that random number and select the next in sequence for the purpose of re-scaling.

(8) Winning Number Draw***.[~~:~~]*** The winning number selection shall only be produced from sold bearer ticket numbers from the current drawing to be available for selection.

(a) Each valid, sold raffle number shall be available for random selection at the initiation of each drawing; and

(b) For raffles ***that [~~which~~]*** offer multiple awards or drawings with separate buy-ins for each, the winning number selection shall only be produced from sold bearer ticket numbers corresponding with each applicable award or drawing. As winning numbers are drawn, they shall be immediately used as governed by the rules of the raffle (***[~~i.e.~~]*** the bearer tickets ***shall not [~~are not to~~]*** be discarded due to adaptive behavior).

(9) No Corruption from Associated Equipment***.[~~:~~]*** An electronic raffle system shall use appropriate protocols to protect the random number generator and random selection process from influence by associated equipment, which may be communicating with the electronic raffle system.

Section 9. Electronic Raffle System Server Requirements***.*** (1) The Electronic Raffle System Server(s) may be located locally, within a single facility or may be remotely located outside of the facility through a Wide Area Network (WAN).

(2) Physical Security***.[~~:~~]*** The servers shall be housed in a secure location that has sufficient physical protection against alteration, tampering***,*** or unauthorized access.

(3) Logical Access Control***.[~~:~~]*** The electronic raffle system shall be logically secured through the use of passwords, biometrics, or other means certified as secure by the independent testing lab. The storage of passwords, PINs, biometrics, and other authentication credentials shall be secure. The system ***shall [~~must~~]***have multiple security access levels to control and restrict different classes of access to the electronic raffle system.

(4) Security from Alteration, Tampering***,[~~,~~]*** or Unauthorized Access***.[~~:~~]***The electronic raffle system shall provide a logical means for securing the raffle data against alteration, tampering, or unauthorized access. The following rules also apply to the raffle data within the Electronic Raffle System:

(a) ***Equipment shall not [~~No equipment shall~~]*** have a mechanism whereby an error will cause the raffle data to automatically clear. Data shall be maintained at all times regardless of whether the server is being supplied with power.

(b) Data shall be stored in ***[~~such~~]*** a way as to prevent the loss of the data when replacing parts or modules during normal maintenance.

(5) Data Alteration***.[~~:~~]*** The electronic raffle system shall not permit the alteration of any accounting, reporting, or significant event data without supervised access controls. In the event any data is changed, the following information shall be documented or logged:

(a) Data element altered;

(b) Data element value prior to alteration;

(c) Data element value after alteration;

(d) Time and date of alteration; and

(e) User login to identify the personnel that performed the alteration.

(6) Server Programming***.[~~:~~]*** There shall be no means available for an operator to conduct programming on the server in any configuration (***[~~e.g.~~]*** the operator ***shall [~~should~~]*** not be able to perform SQL statements to modify the database). ***[~~However,~~]*** Network administrators may perform authorized network infrastructure maintenance with sufficient access rights, which include the use of SQL statements that were already resident on the system.

(7) Copy Protection***.[~~:~~]*** Copy protection to prevent unauthorized duplication or modification of software, for servers or RSUs, may be implemented ***if [~~provided that~~]***:

(a) The method of copy protection is fully documented and provided to the Test Laboratory, ***which shall [~~who will~~]*** verify that the protection works as described; or

(b) The program or component involved in enforcing the copy protection ***may [~~can~~]*** be individually verified by the methodology described in subsection (17).

(8) Uninterruptible Power Supply Support***.[~~:~~] If [~~Where~~]*** the server is a stand-alone application, it ***shall [~~must~~]*** have an uninterruptible power supply (***[~~"~~]***UPS***[~~"~~]***) connected and of sufficient capacity to permit a graceful shut-down and that retains all electronic raffle system data during a power loss. The electronic raffle system server may be a component of a network that is supported by a network-wide UPS ***if [~~provided that~~]*** the server is included as a device protected by the UPS.

(9) System Clock Requirements***.[~~:~~]*** An Electronic Raffle System ***shall [~~must~~]*** maintain an internal clock that reflects the current date and time (in twenty-four (24) hour format showing hours and minutes) that shall be used to provide for the following:

(a) Time stamping of significant events;

(b) Reference clock for reporting; and

(c) Time stamping of all sales and draw events.

(10) System Clock Synchronization Feature***.[~~:~~]*** If multiple clocks are supported the system shall have a facility to synchronize clocks within all system components.

(11) RSU Management Functionality***.[~~:~~]*** An electronic raffle system ***shall [~~must~~]*** have a master list of each authorized RSU in operation, including at minimum the following information for each entry:

(a) A unique RSU identification number or corresponding hardware identifier (***[~~i.e.~~]*** MAC);

(b) Operator identification; and

(c) Tickets issued for sale, if applicable.

(12) RSU Validation***.[~~:~~]*** It is recommended that RSUs be validated at least once per year with at least one ***(1)*** method of authentication. The system shall have the ability to remotely disable the RSU after the threshold of unsuccessful validation attempts has been reached.

(13) Counterfoil Printers***.[~~:~~] If [~~Where~~]*** printed counterfoils are in use, the printer mechanism shall be able to detect and indicate the following error conditions:

(a) Out of paper***;[~~:~~]***

(b) Paper low;***[~~;~~]***

(c) Memory Error;

(d) Printer failure; and

(e) Printer disconnected.

(14) Printer Disable. At any time during an active draw, the operator shall 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.

(15) Significant Event Logging. Significant events shall be communicated and logged on the electronic raffle system, which shall 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) Counterfoil Printer errors:

1. Out of paper ***or [~~/~~]***paper low;

2. Printer disconnect ***or [~~/~~]***failure; and

3. Printer memory error***;[~~.~~]***

(d) Establishment and failure of communications between sensitive electronic raffle system components***;[~~.~~]***

(e) Significant event buffer full;

(f) Program error or authentication mismatch;

(g) Firewall audit log full, ***if [~~where~~]*** supported; and

(h) Remote access, ***if [~~where~~]*** supported.

(16) Significant Event Surveillance or Security Functionality. Each significant event conveyed to the electronic raffle system shall be stored. An electronic raffle system shall provide an interrogation program that enables on-line comprehensive searching of the significant events through recorded data. The interrogation program shall have the ability to perform a search based at least on the following:

(a) Date and time range;

(b) Unique component identification number; and

(c) Significant event identifier.

(17) Storage Medium Backup***.[~~:~~]*** The electronic raffle system shall have sufficient redundancy and modularity so that if any single component or part of a component fails, the raffle ***may [~~can~~]*** continue. Redundant copies of critical data shall be kept on the electronic raffle system with open support for backups and restoration.

(a) All storage shall be through an error checking, nonvolatile physical medium, or an equivalent architectural implementation, so ***if [~~that should~~]*** the primary storage medium fail, the functions of the electronic raffle system and the process of auditing those functions ***may [~~can~~]*** continue with no critical data loss.

(b) The database shall be stored on redundant media so that no single failure of any portion of the system would cause the loss or corruption of data.

(18) Recovery Requirements. In the event of a catastrophic failure***, and if [~~when~~]*** the electronic raffle system cannot be restarted in any other way, it shall be possible to reload the electronic raffle system 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***[~~, etc.~~]***

(19) Verification of System Software. System software components and modules shall be verifiable by a secure means at the system level denoting the program identification and version. The system shall have the ability to allow for an independent integrity check of the components and modules from an outside source and is required for all software that may affect the integrity of the system. This ***shall [~~must~~]*** be accomplished by being authenticated by a third-party device, or by allowing for removal of the media ***so [~~such~~]*** that it ***may [~~can~~]*** be verified externally. This integrity check shall provide a means for field verification of the system components and modules to identify and validate the programs or files. The independent testing laboratory, prior to system approval, shall approve the integrity check method.

Section 10. Electronic Raffle System Communication Requirements. (1) Communication Protocol***.[~~:~~]*** Each component of an electronic raffle system ***shall [~~must~~]*** function as indicated by the communication protocol implemented. An electronic raffle system ***shall [~~must~~]*** provide for the following:

(a) Communication between all system components ***and shall [~~must~~]*** provide mutual authentication between the component and the server***;[~~.~~]***

(b) All protocols ***shall [~~must~~]*** use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent eavesdropping and tampering. Any alternative implementations ***shall [~~will~~]*** be reviewed on a case-by-case basis, with regulatory approval; and

(c) All data communications critical to the raffle shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication.

(2) Connectivity***.[~~:~~]*** Only authorized devices shall be permitted to establish communications between any system components. Electronic raffle systems shall provide a method to:

(a) Verify that the system component is being operated by an authorized user;

(b) Enroll and un-enroll system components;

(c) Enable and disable specific system components***;[~~.~~]***

(d) Ensure that only enrolled and enabled system components participate in the raffle; and

(e) Ensure that the default condition for components shall be un-enrolled and disabled.

(3) Loss of Communications***.[~~:~~]*** Raffle sales units (RSUs) may continue to sell tickets when not in communication with the system. Sales taking place on the RSU during a loss of communication with the system shall be logged on the device. The RSU shall deactivate upon detecting the limit of its buffer overflow. Upon the re-establishment of communication, the system shall require the RSU to re-authenticate with the server(s). All tickets sold during communication loss shall be transmitted to the system. Loss of communications shall not affect the integrity of critical memory.

(4) System Security***.[~~:~~]***All communications, including remote access, ***shall [~~must~~]*** pass through at least one ***(1)*** approved application-level firewall and ***shall [~~must~~]*** not have a facility that allows for an alternate network path. Any alternate network path existing for redundancy purposes ***shall [~~must~~]*** also pass through at least one ***(1)*** application-level firewall.

(5) Firewall Audit Logs. The firewall application ***shall [~~must~~]*** maintain an audit log and ***shall [~~must~~]*** disable all communications and generate a significant event ***that [~~which~~]*** meets the requirements as specified in Section 9(13) if the audit log becomes full. The audit log shall contain:

(a) All changes to configuration of the firewall;

(b) All successful and unsuccessful connection attempts through the firewall; and

(c) The source and destination IP Addresses, Port Numbers***,*** and MAC Addresses.

(6) Remote Access. ***[~~"Remote access" means any access from outside the system or system network including any access from other networks within the same establishment.~~]*** The electronic raffle system shall have the option to disable remote access. Remote access shall accept only the remote connections permissible by the firewall application and electronic raffle system settings. In addition, there shall be:

(a) No unauthorized remote user administration functionality, such as adding users, or changing permissions;

(b) No unauthorized access to any database other than information retrieval using existing functions;

(c) No unauthorized access to the operating system; and

(d) For systems using an electronic random number generator, the electronic raffle system ***shall [~~must~~]***immediately detect remote access.

(7) The system manufacturer may, as needed, remotely access the electronic raffle system and its associated components for the purpose of product and user support.***[~~.~~]***

(8) Remote Access Auditing. The electronic raffle system ***shall [~~must~~]*** maintain an activity log ***that [~~which~~]*** updates automatically depicting all remote access information, to include:

(a) Log on name;

(b) Time and date the connection was made;

(c) Duration of connection; and

(d) Activity while logged in, including the specific areas accessed and changes that were made.

(9) Wide Area Network (***[~~“~~]***WAN***[~~”~~]***) communications are permitted as allowed by the regulatory body and shall meet the following requirements:

(a) The communications over the WAN are secured from intrusion, interference***,*** and eavesdropping via techniques such as use of a Virtual Private Network (VPN) or encryption; and

(b) Only functions documented in the communications protocol shall be used over the WAN. The protocol specification shall be provided to the Testing Laboratory.

(10) Wireless Network Communications. If a wireless communication solution is utilized, it shall adhere to the following requirements:

(a) Segregation of Networks. Networks used by the electronic raffle systems ***shall [~~should~~]*** be separate and not include other devices that are not part of the electronic raffle system.

(b) Service Set Identifier (SSID). The wireless network name (SSID) used to identify the wireless network ***shall [~~should~~]*** be hidden and not broadcast.

(c) Media Access Control (MAC) Address Filtering. The wireless network should use MAC address filtering ***[~~as means~~]*** to validate whether or not a device may connect to the wireless network.

(d) Device Registration. The electronic raffle system ***shall [~~should~~]*** use a device registration method ***[~~as means~~]*** to validate whether or not a device is an authorized device on the electronic raffle system.

Section 11. Online Raffle Ticket Sales. (1) All systems used for the sale of raffle tickets through the Internet ***shall [~~must~~]*** meet the requirements contained within this ***administrative regulation [~~document~~]*** and the terms and conditions set forth by ***this administrative regulation [~~these regulations~~]*** for the sale of raffle tickets through the Internet.

[~~(2) Definitions:~~

~~(a) “Access control” means the restriction of access to a place or other resource. Locks and login credentials are two mechanisms of access control.~~

~~(b) “Address Resolution Protocol (‘ARP’)” is the protocol used to translate IP addresses into MAC addresses to support communication on a LAN (“Local Area Network”). The Address Resolution Protocol is a request and reply protocol and it is communicated within the boundaries of a single network, never routed across internetwork nodes (connection points, either a redistribution point or an end point for data transmissions).~~

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

~~(d) “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.~~

~~(e) “Bi-Directional” means the ability to move, transfer or transmit in both directions.~~

~~(f) “Counterfoil” means an electronic record or paper ticket stub, also known as a barrel ticket, which will be drawn to determine a winner and contains a player's draw number matching the bearer ticket purchased and may, depending on the type of raffle, contain the name, address, or telephone number of the player.~~

~~(g) “Crypto-analytic” means an attack against the encryption key (refer to definition of encryption key).~~

~~(h) “Cryptographic” means anything written in a secret code, cipher, or the like.~~

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

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

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

~~(l) “Encryption key” means a sequence of numbers used to encrypt or decrypt (to decode/decipher) data.~~

~~(m) “Firewall” means any number of security schemes that prevent unauthorized users from gaining access to a computer network or that monitor transfers of information to and from the network.~~

~~(n) “Geolocation” means identifying the real-world geographic location of an Internet connected computer, mobile device, or website visitor.~~

~~(o) “Host” means a computer system that is accessed by a user working at a remote location. Typically, the term is used when there are two computer systems connected by modems and telephone lines. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal. A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.~~

~~(p) “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 should take in response to various commands.~~

~~(q) “Internet” means an interconnected system of networks that connects computers around the world via the TCP/IP protocol. TCP/IP protocol is short for Transmission Control Protocol/Internet Protocol, the suite of communications protocols used to connect hosts on the Internet.~~

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

~~(s) “Internet Protocol (‘IP’)” means an identifier for a computer or device on a TCP/IP network.~~

~~(t) “Media Access Control (‘MAC’)” means hardware address that uniquely identifies each node, such as computer or printer, of a network.~~

~~(u) “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.~~

~~(v) “Message authentication” means a security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.~~

~~(w) “Online” means being connected to the Internet.~~

~~(x) “Online Purchasing Platform” means the raffle system hardware and software which drives the features common to all raffles offered, and which forms the primary interface to the Raffle System for both the patron and the operator. The online purchasing platform provides the patron with the means to register an account, log in to/out of their account, modify their account information, make ticket purchases, request account activity statement/reports, and close their account. In addition, any web pages displayed to the patron that relate to ticket purchasing offered on the raffle system. The online purchasing platform provides the operator with the means to review patron accounts, enable or disable raffles, generate various financial transaction and account reports, input raffle outcomes, enable or disable patron accounts, and set any configurable parameters.~~

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

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

~~(aa) “Security certificate” means information, often stored as a text file, which is used by the Secure Socket Layers (“SSL”) protocol to establish a secure connection. A security certificate contains information about whom it belongs to, who it was issued by, valid dates, a unique serial number or other unique identification that can be used to verify the contents of the certificate. In order for an SSL connection to be created, both sides must have a valid security certificate, which is also called a digital ID.~~

~~(ab) “Stateful firewall” means a firewall that keeps track of the state of network connections traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected. Stateful inspection, also referred to as Dynamic Packet Filtering, is a security feature often included in business networks,~~

~~(ac) “Stateless” means a communications protocol 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. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. In contrast, a protocol which requires the keeping of internal state is known as a stateful protocol. Examples of stateless protocols include Internet Protocol (IP) and the Hypertext Transfer Protocol (HTTP).~~]

(2) All online raffle ticket sales systems, software***,*** and database requirements ***shall [~~must~~]*** be tested and certified by an independent testing laboratory to meet the applicable requirements set forth in this ***administrative regulation [~~document~~]*** and approved by the department.

(3) Operation manuals and service manuals ***shall [~~must~~]*** be expressed in broad terms that are directly relevant to the system used to sell raffle ticket(s) through the Internet and ***shall [~~must~~]*** be provided at the request of the department.

(4) Geolocation***.[~~:~~]*** The raffle system, online purchasing platform or the patron device ***shall [~~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.

(5) Inventory***.[~~:~~] If [~~When~~]*** issued a charitable gaming license to conduct a raffle, the charitable organization shall provide the number of raffle tickets available for sale through the

Internet. The raffle system software shall have the ability to set time limits for which tickets may be purchased. Upon completion of the sale of the final raffle ticket for a charitable organization raffle, the raffle ***shall [~~must~~]***close.

(6) Systems used by the purchaser to obtain raffle ticket(s) through the Internet ***shall [~~must~~]*** be designed to be reasonably impervious to communication errors. Personally identifiable information, sensitive account data***,*** and financial information shall be protected over a public network.

(7) Asset Management***.[~~:~~]*** All assets housing, processing of communication controlled information, including those comprising the operating environment of the Raffle system ***[~~and/~~]***or its components, ***shall [~~should~~]*** be accounted for and have a designated ***[~~“~~]***owner***[~~”~~]*** responsible for ensuring that information and assets are appropriately classified, and defining and periodically reviewing access restrictions and classifications.

(8) Raffle Equipment Security***.[~~:~~]*** Raffle system servers ***shall [~~must~~]*** be located in server rooms ***that [~~which~~]*** restrict unauthorized access. Raffle system servers shall be housed in racks located within a secure area.

(9) Network Security Management***.[~~:~~]***To ensure purchasers are not exposed to unnecessary security risks by choosing to participate in raffles, these security requirements ***shall [~~must~~]*** apply to the following critical components of the raffle system:

(a) Raffle system components ***that [~~which~~]*** record, store, process, share, transmit***,*** or retrieve sensitive purchaser information, ***such as [~~e.g.~~]*** credit card ***or [~~/~~]***debit card details, authentication information, ***or*** patron account balances;

(b) Raffle system components ***that [~~which~~]*** store results of the current state of a purchaser’s purchase order;

(c) Points of entry to and exit from the above systems (other systems ***that [~~which~~]*** are able to communicate directly with the core critical systems); and

(d) Communication networks ***that [~~which~~]*** transmit sensitive patron information.

(10) Networks should be logically separated ***so [~~such~~]*** that there ***shall [~~should~~]*** be no network traffic on a network link ***that [~~which~~]*** cannot be serviced by hosts on that link.

(a) The failure of any single item ***shall [~~should~~]*** not result in denial of service;

(b) An Intrusion Detection System ***or [~~/~~]***Intrusion Prevention System ***shall [~~must~~]*** be installed on the network ***and shall[~~which can~~]***:

1. Listen to both internal and external communications;

2. Detect or prevent Distributed Denial of Services (***[~~“~~]***DDoS***[~~”~~]***) attacks;

3. Detect or prevent shellcode from traversing the network;

4. Detect or prevent Address Resolution Protocol (***[~~“~~]***ARP***[~~”~~]***) spoofing; and

5. Detect other Man-in-the-Middle indicators and server communications immediately if detected.

(c) Stateless protocols ***shall [~~should~~]*** not be used for sensitive data without stateful transport (HTTP is allowed if it runs on TCP)***;[~~.~~]***

(d) All changes to network infrastructure ***shall [~~must~~]*** be logged;

(e) Virus scanners or detection programs ***shall [~~should~~]*** be installed on all pertinent information systems. These programs shall be updated regularly to scan for new strains of viruses;

(f) Network security shall be tested by a qualified and experienced individual at least once per year; ***[~~and~~]***

(g) Testing shall include testing of the external (public) interfaces and the internal network***; and[~~.~~]***

(h) Testing of each security domain on the internal network shall be undertaken separately.

(11) Communication Protocol***.[~~:~~]*** Online raffle tickets offered for sale by a charitable organization shall support a defined communication protocol that ensures purchasers are not exposed to unnecessary security risks when using the Internet for this purpose. Each component of a raffle system ***shall [~~must~~]*** function as indicated by the communication protocol implemented. The system ***shall [~~must~~]*** provide for the following:

(a) All critical data communication shall be protocol based or incorporate an error detection and correction scheme to ensure accuracy of messages received;

(b) All critical data communication shall employ encryption. The encryption algorithm shall employ variable keys or similar methodology to preserve secure communication;

(c) Communication between all system components ***shall [~~must~~]*** provide mutual authentication between the component and the server;

(d) All protocols shall use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent eavesdropping and tampering***;[~~.~~]***

(e) All data communications critical to raffle ticket sales through the Internet shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication.

(12) Remote Access***.[~~:~~] [~~Remote access means any access from outside the system or system network including any access from other networks within the same establishment.~~]*** Remote access shall only be allowed with prior written approval of the department and shall have the option to be disabled. ***If [~~Where~~]*** allowed, remote access shall accept only the remote connections permissible by the firewall application and online raffle ticket sales settings. In addition, there shall be:

(a) No authorized remote user administration functionality;

(b) No authorized access to any database other than information retrieval using existing functions;

(c) No authorized access to the operating system; and

(d) The raffle system ***shall [~~must~~]*** maintain an activity log ***that [~~which~~]*** updates automatically depicting all remote access information.

(13) Error Recovery***.[~~:~~]*** The system used by a licensed charitable organization to offer the sale of raffle ticket(s) through the Internet ***shall [~~must~~]*** be able to recover messages when they are received in error. This would include inaccurately inputting personal ***or [~~/~~]***banking information ***that [~~which~~]*** would result in the purchaser being notified that the information is invalid and ***shall [~~must~~]*** require review and corrective measures. In the event of a catastrophic failure***, if [~~when~~]*** the system cannot be restarted in any other way, it shall be possible to reload the system information from the last viable backup point and fully recover the contents of that backup, including***[~~, but not limited to~~]***:

(a) Significant events;

(b) Accounting information;

(c) Reporting information; and

(d) Specific site information, including ***[~~but not limited to~~]*** employees file and the raffle set-up.

(14) Bi-Directional Requirements***.[~~:~~]*** Any system used to sell raffle ticket(s) through the Internet shall be tested by an independent testing laboratory, ***which [~~who~~]*** shall certify 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.

(15) Encryption***.[~~:~~]*** Security messages that traverse data communications lines ***shall [~~must~~]*** be encrypted using an encryption key or keys to ensure that communications are demonstrably secure against crypto-analytic attacks. The encryption keys or keys used to provide security to the system that provide for the sale of raffle tickets through the Internet ***shall [~~must~~]*** be monitored and maintained. Additionally, there ***shall [~~must~~]*** be a documented process for:

(a) Obtaining or generating encryption keys;

(b) Managing the expiry of encryption keys ***[~~if encryption keys~~]***;

(c) Revoking encryption keys;

(d) Securely changing the current encryption keyset;

(e) The storage of any encryption keys; and

(f) To recover data encrypted with a revoked or expired encryption key for a defined period of time after the encryption key becomes valid.

(16) Cryptographic Controls***.[~~:~~]*** Cryptographic controls shall be implemented for the protection of the following information:

(a) Any sensitive or personally identifiable information shall be encrypted if it traverses a network with a lower level of trust;

(b) Data that is not required to be hidden ***and has to [~~but must~~]*** be authenticated shall use some form of message authentication technique;

(c) Authentication ***shall [~~must~~]*** use a security certificate **[~~from an organization~~]** approved by the independent testing laboratory;

(d) The grade of encryption used ***shall [~~should~~]*** be appropriate to the sensitivity of the data;

(e) The use of encryption algorithms shall be reviewed periodically by qualified management staff to verify that the current encryption algorithms are secure;

(f) Changes to encryption algorithms to correct weaknesses shall be implemented as soon as practical. If no ***[~~such~~]*** changes are available, the algorithm shall be replaced; and

(g) Encryption keys ***shall [~~must~~]*** not be stored without being encrypted themselves through a different encryption method ***[~~and/~~]***or by using a different encryption key.

(17) Firewalls. All online raffle systems shall utilize firewalls that comply with the following provisions:

(a) A firewall shall be located at the boundary of any two ***(2)*** dissimilar security domains.

(b) All connections to hosts used for the sale of raffle tickets through the Internet shall be housed in a secure data center and ***shall [~~must~~]*** pass through at least one ***(1)*** application-level firewall. This includes connections to and from any non-related hosts used by the operator.

(c) The firewall shall be a separate hardware device with the following characteristics:

1. Only firewall-related applications may reside on the firewall; and

2. Only a limited number of accounts may be present on the firewall.

(d) The firewall shall reject all connections except those that have been specifically approved.

(e) The firewall shall reject all connections from destinations ***that [~~which~~]*** cannot reside on the network from which the message originated.

(f) The firewall shall maintain an audit log of all changes to parameters ***that [~~which~~]*** control the connections permitted through the firewall.

(g) The firewall shall maintain an audit log of all successful and unsuccessful connection attempts. Logs ***shall [~~should~~]*** be kept for ***ninety (***90***)*** days and a sample reviewed monthly for unexpected traffic.

(h) The firewall shall disable all communication if the audit log becomes full.

(18) Firewall Audit Logs***.[~~:~~]*** The audit log shall contain:

(a) All changes to ***the*** configuration of the firewall;

(b) All successful and unsuccessful attempts through the firewall; and

(c) The source and destination IP addresses, port numbers***,*** and MAC addresses.

(19) System Clock***.[~~:~~]***The system used for the sale of raffle tickets through the Internet shall maintain an internal clock that reflects the current date and time that shall be used for the following:

(a) Time stamping of significant events;

(b) Reference clock for reporting; and

(c) Time stamping of all sales.

(20) Purchase Session***.[~~:~~]*** A purchase session consists of all activities and communications performed by a purchaser during the time the purchaser accesses the raffle system or online purchasing platform. Tickets sold online shall only be purchased during a purchase session.

(21) Purchasing Tickets***.[~~:~~]*** A participant may purchase a raffle ticket from the website by following the instructions appearing on the screen and providing payment for the tickets. Each raffle ticket ***shall [~~must~~]*** be sold individually for the price indicated. Multiple discounted prices ***shall [~~will~~]*** only be allowed if a way of ensuring financial accountability is possible by the online purchasing platform or raffle system:

(a) A ticket purchase via a credit card transaction or other methods ***that may [~~which can~~]*** produce a sufficient audit trail ***shall [~~must~~]*** not be processed until ***[~~such time as~~]*** the funds are received from the issuer or the issuer provides an authorization number indicating that the purchase has been authorized;

(b) There ***shall [~~must~~]*** be a clear notification that the purchase has been accepted by the system and the details of the actual purchase accepted ***shall [~~must~~]*** be provided to the patron once the purchase is accepted; and

(c) Purchase confirmation shall include the amount of the purchase accepted by the raffle system or online purchasing platform.

(22) Disputes***.[~~:~~]*** The raffle system or online purchasing platform ***shall [~~must~~]*** conspicuously provide a mechanism to advise the patron of the right to make a complaint against the operator and to enable the patron to notify the department of ***[~~such~~]*** a complaint.

(23) Bearer Ticket Issuance***.[~~:~~]*** After the payment of a fee, the purchaser shall receive a receipt through the Internet that the purchase of a raffle ticket or tickets is complete. Upon receiving the receipt acknowledging the purchase through the Internet, the purchaser may receive the raffle ticket via e-mail. The receipt acknowledging purchase and the issuance of the raffle tickets through the Internet ***shall [~~must~~]*** be processed as two (2) separate transactions.

(24) Validation Numbers***.[~~:~~]*** The method used by the raffle system to generate the bearer ticket validation number ***shall [~~must~~]*** be unpredictable and ensure against duplicate validation numbers for the raffle currently in progress.

(25) Voiding a Ticket***.[~~:~~]*** If a ticket is voided, the appropriate information shall be recorded, which includes the draw numbers and the validation number pertaining to the voided ticket. Voided draw numbers shall not be able to be resold or reissued.

(26) Raffle Drawing Requirements***.*** (a) A raffle drawing shall be held the date, time, and place stated on the organization's license or certificate of exemption.

(b) The operator shall conduct a manual or electronic draw procedure ***that [~~which~~]*** ensures a randomly selected draw number as a winner from all the tickets sold. Each drawn counterfoil shall be verified as a sold and valid ticket. Voided tickets shall not be qualified toward any prize. This process shall be repeated for each advertised prize.

(c) Results of the drawing become official and final after the drawn number is verified as a winning raffle ticket for the respective drawing and is presented to the participants for the raffle. The winning draw number shall be made available on the raffle website for the participants to review. Operators may utilize any additional methods in presenting the winning draw number(s) to the participants.

(27) Accounting Requirements***.[~~:~~]*** Any system used for the sale of raffle tickets through the Internet ***shall [~~must~~]*** have the capability to log sales and to print reports detailing sales and accounting information for specific dates and time periods ***that shall [~~must~~]*** be available. This information shall include***[~~, but is not limited to,~~]*** the price of each raffle ticket, number of raffle tickets sold, and total sales. The system or other equipment shall be capable of producing accounting reports to include the following information:

(a) Data required to be maintained for each raffle drawing, including:

1. Date and time of event;

2. Organization running the event;

3. Sales information;

4. Value of prize(s) awarded;

5. Prize distribution;

6. Refund totals of event***;***

7. Draw numbers-in-play;

8. Winning number(s) drawn (including draw order, call time***,*** and claim status); and

9. Any other information required by 820 KAR 1:057.

(b) Exception Report***.[~~:~~]*** A report ***that [~~which~~]*** includes system exception information, including***[~~, but not limited to,~~]*** changes to system parameters, corrections, overrides***,*** and voids.

(c) Bearer Tickets Reports***.[~~:~~]*** A report ***that [~~which~~]*** includes a list of all bearer tickets sold including all associated draw numbers and selling price.

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

(e) Voided Draw Number Report***.[~~:~~]***A report ***that [~~which~~]*** includes a list of all draw numbers that have been voided including corresponding validation numbers.

(f) Event Log***.[~~:~~]***A report ***that [~~which~~]*** lists all events recorded specific to the sales of raffle ticket(s) through the Internet. This ***shall [~~will~~]*** include the date and time of the transaction and a brief description of the transaction ***[~~and/~~]***or identifying code.

(g) Corruption Log***.[~~:~~]***A report ***that [~~which~~]*** lists all Internet transactions that were unable to be reconciled to the system.

(28) Sales and Accounting Report Requirements***.[~~:~~]*** Any raffle ticket sold ***shall [~~must~~]*** be included in the sales and accounting reports and be detailed in all financial transactions on the system. In addition, a log relating to accounting and raffle ticket sales ***shall [~~must~~]*** be maintained on the system. The charitable organization conducting the raffle shall be given the option of printing this log on demand.

(29) Backup Requirements***.[~~:~~]***Any system used for the sale of raffle ticket(s) through the Internet ***shall [~~must~~]*** have a backup and archive utility to allow the licensed charitable organization, conducting the raffle, the ability to save critical data ***if [~~should~~]*** a system failure occurs. This backup ***may [~~can~~]*** be automatically run by the charitable organization.

(30) Data Alteration***.[~~:~~]*** The alteration of any accounting, reporting or significant event data related to the sale of raffle tickets through the Internet shall include supervised access controls. In the event any data is changed, the following information shall be logged, documented, stored***,*** and available upon request for review:

(a) Data element altered;

(b) Data element value prior to alteration;

(c) Data element value after alteration;

(d) Time and date of alteration; and

(e) User login of the personnel that performed the alteration.

(31) Access Controls***.[~~:~~]*** The allocation of access privileges shall be restricted and controlled on business requirements and the principle of least privilege.

(a) A formal user registration and de-registration procedure ***shall [~~must~~]*** be in place for granting and revoking access to all information systems and services.

(b) All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

(c) The use of generic accounts shall be limited, and ***if [~~where~~]*** used ***the [~~for~~]*** reasons for their use shall be formally documented.

(d) Password provision ***shall [~~must~~]*** be controlled through a formal management process.

(e) Passwords ***shall [~~must~~]*** meet business requirements for length, complexity***,*** and lifespan.

(f) Access to system applications shall be controlled by a secure log-on procedure.

(g) Appropriate authentication methods, in addition to passwords, shall be used to control access by remote users

(h) Any physical access to areas housing components used for the sale of raffle ticket(s) through the Internet application and any logical access to these applications ***shall [~~must~~]*** be recorded.

(i) The use of automated equipment identification to authenticate connections from specific locations and equipment shall be formally documented and ***shall [~~must~~]*** be included in the regular review of access by management.

(j) Restrictions on connection times shall be used to provide additional security for high-risk applications.

(k) The use of utility programs that might be capable of overriding system application controls shall be restricted and tightly controlled.

(l) A formal policy shall be in place and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

(32) Purchaser Account Registration***.[~~:~~]*** The raffle system or online purchasing platform ***shall [~~must~~]*** employ a mechanism to collect purchaser information prior to registration of a purchaser account. The purchaser ***shall [~~must~~]*** be fully registered, and the purchaser's account ***shall [~~must~~]*** be activated prior to permitting ticket purchases. Once the identity verification is successfully complete, and the purchaser has acknowledged all of the necessary privacy policies and the terms and conditions, the purchaser account registration is complete and the patron account ***shall [~~can~~]*** become active.

(33) Third***-***Party Services***.[~~:~~]*** Any third-party service providers contracted to provide service involving accessing, processing, communicating***,*** or managing the sale of raffle tickets through the Internet ***shall [~~must~~]***adhere to information contained in this ***administrative regulation [~~document~~]***. The security roles and responsibilities of third***-***party service providers ***shall [~~should~~]*** be defined and documented as it relates to the security of information.

(a) Agreements with third***-***party service providers involving accessing, processing, communicating***,*** or managing the purchase of on-line raffle tickets through the Internet***[~~/~~]***or its components, or adding products or services to the system used***[~~/~~]***or its components shall cover all relevant security requirements.

(b) The services, reports***,*** and records provided by the third***-***party shall be monitored and reviewed by the department upon request.

(c) Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

(d) The access rights of third-party service providers to the system ***[~~and/~~]***or its components shall be removed upon termination of their contract or agreement, or adjusted upon change.

CONTACT PERSON: Doug Hardin, Staff Attorney, Department of Charitable Gaming, 500 Mero Street 2NW24, Frankfort, Kentucky 40601; phone (502) 782-8204; fax (502) 573-6625; doug.hardin@ky.gov.