Sec. 12-865-13. Electronic Wagering Platform Requirements

(a) The provisions of this section apply to all electronic wagering platforms used by an online gaming operator to offer any of the following, directly or through a sports wagering retailer:

(1) Interactive online games;

(2) Retail sports wagering:

(3) Online keno; and

(4) Online lottery.

(b) All equipment for an electronic wagering platform under this section, except equipment used exclusively for fantasy contests, shall be located as follows:

(1) Hardware shall be located in a facility owned or leased by the online gaming operator that is secure, inaccessible to the public, and specifically designed to house that equipment, and where the equipment shall be under the control of the online gaming operator, within the state or located as permitted under subsection (bb) of this section; and

(2) Hardware and any backup hardware for an electronic wagering platform used solely to operate fantasy contests is not required to be located within the State of Connecticut.

(c) Online gaming operators shall take commercially reasonable steps to ensure that redundancy protocols are adopted in the event electronic wagering platform outages occur. Such steps shall include that the backup hardware is located in a secure facility, inaccessible to the public and located in the state. The Department may permit backup hardware for the operation of online lottery and online keno to be located outside of the state if an appropriate location is approved by the department in writing, which approval shall be at the commissioner's discretion and not subject to administrative appeal. The online gaming operator shall ensure the department has access to the physical location where the server is housed within six hours of a request by the department, which access shall be reflected in the agreement between the online gaming operator and the cloud-based server host.

(d) The online gaming operator shall provide access to electronic wagering platform related data considered necessary by the department and in a manner approved by the department. For electronic wagering systems operating online lottery and keno, the online gaming operator shall give the department the ability to independently monitor the electronic wagering platform transactions and reporting related to online lottery and keno.

(e) An electronic wagering platform used for operating online keno and online lottery shall also comply with the provisions set forth in sections 12-865-17 and 12-865-21 of the Regulations of Connecticut State Agencies.

(f) Electronic wagering platforms shall require a patron after fifteen minutes of user inactivity, as measured by the electronic wagering platform, to re-enter his or her username and password manually or through biometric authentication, including fingerprint, facial or voice recognition, or any other method approved by the department.

(g) Each online gaming operator offering internet gaming shall comply with the data privacy provisions of section 12-865-32 and the cybersecurity provisions of section 12-865-33 of the Regulations of Connecticut State Agencies and shall perform an annual system integrity and security assessment conducted by an independent security professional selected by the licensee and licensed by the department as an online gaming service provider. The independent professional's report on the assessment shall be submitted to the department

annually within thirty days of submission of the report to the licensee and shall include:

(1) Scope of review;

(2) Name and company affiliation of the individual or individuals who conducted the assessment;

(3) Date of the assessment;

(4) Findings;

(5) Recommended corrective action, if applicable; and

(6) Licensee's response to the findings and recommended corrective action.

(h) An electronic wagering platform shall utilize sufficient security to ensure patron access is appropriately limited to the account holder. Unless otherwise authorized by the department, security measures shall include at a minimum:

(1) A username;

(2) Compliance with NIST Special Publication 800-63-3 "Digital Identity Guidelines" for password and access security including requiring two of the three multi-factor identification methods, which include a (i) strong alphanumerical password; (ii) fingerprint or other biometric data; and (iii) cryptographic key by SMS or electronic mail verification, or other requirements set forth by the department under section 12-865-3(n) of the Regulations of Connecticut State Agencies; and

(3) Electronic notification to the patron's registered electronic mailing address, cellular phone or other device each time an internet gaming account is accessed, except that a patron may opt out of such notification.

(i) An electronic wagering platform shall be designed to detect and report:

(1) Suspicious behavior, such as cheating, theft, embezzlement, collusion, money laundering, or any other illegal activities; and

(2) The creation of an account by an excluded person or any individual who is prohibited from any form of internet gaming.

(j) Internet gaming account access information shall not be permanently stored on a patron device that is provided for patron use at a sport wagering retailer facility. Such information shall be masked after entry, encrypted immediately after entry is complete, and may be temporarily stored or buffered during patron entry provided that the buffer is automatically cleared as follows:

(1) After the patron confirms that the account access entry is complete; or

(2) If the patron fails to complete the account access entry within one minute.

(k) Unless otherwise approved by the department, an electronic wagering platform shall associate a patron's account with a single patron device during each patron session.

(*l*) Each patron session shall have a unique identifier assigned by the electronic wagering platform.

(m) The electronic wagering platform shall immediately terminate a patron session whenever:

(1) Required by the department or licensee;

(2) The patron ends a session;

(3) The patron logs onto the system from another patron device;

(4) The patron fails more than once any authentication during a game or patron session; or

(5) A system error impacts game play.

(n) Electronic wagering platforms shall employ a mechanism that can detect and prevent any patron initiated wagering or withdrawal activity that would result in a negative balance of an internet gaming account.

(o) Electronic wagering platforms shall disable a patron's account after three failed log in attempts and require strong authentication to recover or reset a password or username.

(p) An electronic wagering platform shall allow a patron to establish responsible gaming limits. Any change making the limits more restrictive shall be effective no later than the patron's next log in. Any change making the limits less restrictive shall become effective only after the time limit previously established by the patron has expired and the patron reaffirms the requested change. Responsible gaming limit options offered to patrons shall include, but are not limited to, the following:

(1) A deposit limit shall be offered on a daily, weekly, and monthly basis and shall specify the maximum amount of money a patron may deposit into his or her internet gaming account during a particular period of time.

(2) A spend limit shall be offered on a daily, weekly, and monthly basis and shall specify the maximum amount of patron deposits that may be put at risk during a particular period of time.

(3) A time-based limit shall be offered on a daily basis and shall specify the maximum amount of time, measured hourly from the patron's log in to log off, a patron may spend playing on an electronic wagering platform, provided, however, that if the time-based limit is reached a patron will be permitted to complete any round of play.

(q) An electronic wagering platform shall implement automated procedures to identify and prevent the following individuals from placing a wager:

(1) Individuals under the minimum legal age;

(2) Individuals outside of Connecticut;

(3) Individuals on the self-exclusion list;

(4) Patrons who have had their account closed;

(5) Patrons who have had their account suspended;

(6) Patrons who have exceeded their spend or time-based limit; and

(7) Patrons prohibited from placing a wager pursuant to the act, but only with regard to the categories of games that such patrons are prohibited from participating in.

(r) An electronic wagering platform shall provide a patron with the ability to view the outcome and subsequent account balance changes for the previous game, including a game completed subsequent to an outage (for example, network disconnection or patron device malfunction).

(s) Unless otherwise approved by the department, a record of all complimentaries redeemed in the state shall be maintained in an electronic file that is readily available to the department. The master wagering licensee and online gaming operator shall only deduct complimentaries redeemed in the state from gross gaming revenue. All complimentaries shall be stated in clear and unambiguous terms and shall be readily accessible by the patron. Offer terms and the record of all offers for complimentaries shall include at a minimum:

(1) The date and time presented;

(2) The date and time the offer is active and expires; and

(3) Patron eligibility and redemption requirements.

(t) Manual adjustments by a licensee to internet gaming data shall only be made by a software application approved by the department.

(u) When a patron's lifetime deposits exceed $2,500, the electronic wagering platform shall prevent any wagering until the patron acknowledges the following:

(1) The patron has met the department's lifetime gaming deposit threshold of $2,500;

(2) The patron has the capability to establish responsible gaming limits or close the patron's account;

(3) The message "If you or someone you know has a gambling problem and wants help, call (888) 789-7777 or visit ccpg.org/chat," or the equivalent of such message in a language other than English. The department may update the phone number or web address to be displayed by providing ten days' notice to each licensee, after which time the licensee shall display the new number and address. The department shall consult with the Department of Mental Health and Addiction Services prior to revising the required problem gambling message and shall provide ten days' notice to each licensee, after which time the licensee shall display the new message; and

(4) The acknowledgements prescribed in subdivisions (2) and (3) of this subsection shall be required every six months after the patron has met the department's lifetime gaming deposit threshold of $2,500.

(v) Gaming entity licensees may utilize celebrity or other players to participate in peer-to-peer gaming for advertising or publicity purposes. Such players may have their accounts funded in whole or in part or may be paid a fee by a gaming entity licensee. If a celebrity player is utilized and the celebrity player generates winnings or prizes that the gaming entity licensee does not permit the celebrity player to retain, such winnings or prizes shall be included as internet gaming gross revenue in a manner approved by the department.

(w) The system requirements in this section apply to all of the following components of an electronic wagering platform:

(1) Electronic wagering platform components which record, store, process, share, transmit or retrieve confidential information;

(2) Electronic wagering platform components which generate, transmit or process random numbers used to determine the outcome of games or virtual events;

(3) Electronic wagering platform components which store results or the current state of the patron's wager;

(4) Points of entry and exit from the systems described in subdivisions (1) to (3), inclusive, of this subsection or other systems which are able to communicate directly with core critical systems; and

(5) Communication networks which transmit patron information.

(x) An online gaming operator shall not engage in any public facing gaming activity unless its electronic wagering platform has been tested and certified by a licensed independent laboratory as set forth in 12-865-19 of the Regulations of Connecticut State Agencies. Online gaming operators shall comply with the following to obtain authorization from the department to use an electronic wagering platform in the state:

(1) Prior to engaging in any public facing gaming activity, the online gaming operator shall submit an application to the department in the manner and form prescribed by the

department and provide the documentation required under subsection (y) of this section to request authorization for the use of its electronic wagering platform. The department will review the application and make a suitability determination as set forth in section 12-865-19 of the Regulations of Connecticut State Agencies.

(2) The department may require that an electronic wagering platform be re-certified by a licensed independent testing laboratory and the new certification submitted to the department in the event that the department suspects that the integrity of the electronic wagering platform may be vulnerable or compromised.

(3) The online gaming operator is responsible for all costs associated with testing and obtaining certifications or re-certification.

(y) The online gaming operator shall provide all of the following information and any additional information that the department may request:

(1) A complete, comprehensive, and technically accurate description and explanation of the electronic wagering platform and its intended use in both technical and lay language.

(2) Detailed operating procedures or service manuals, or both, of the electronic wagering platform.

(3) A summary description of internet game play, system features, and fault conditions.

(4) Details of all tests performed on the electronic wagering platform, the conditions and standards under which the tests were performed, the test results, and the identity of the individual who conducted each test.

(5) A description of all hardware devices.

(6) A description of all software including software version.

(7) A description of all wagering communications.

(8) A description of all third-party integrated systems.

(9) Any equipment that is required to perform testing.

(10) A description of the risk management framework including, but not limited to:

(A) User access controls for all electronic wagering personnel;

(B) Information regarding segregation of duties;

(C) Information regarding automated risk management procedures;

(D) Information regarding fraud detection;

(E) Controls for ensuring regulatory compliance; and

(F) Anti-money laundering compliance standards.

(z) Electronic wagering platform and internet games technical standards.

(1) Any electronic wagering platform or internet game shall meet or exceed the specifications set forth in sections 12-865-1 to 12-865-34, inclusive, of the Regulations of Connecticut State Agencies and other technical standards established pursuant to section 12-865-3(n) of the Regulations of Connecticut State Agencies. Failure to comply with the approved specifications, internal controls, or technical standards may result in disciplinary action by the department.

(2) Online gaming operators shall meet or exceed the specifications set forth in sections 12-865-1 to 12-865-34, inclusive, of the Regulations of Connecticut State Agencies and any other technical standards established pursuant to section 12-865-3(n) of the Regulations of Connecticut State Agencies.

(3) If the electronic wagering platform meets or exceeds the technical standards adopted

in subdivision (1) of this subsection, the independent testing laboratory shall certify the electronic wagering platform. Online gaming operators are prohibited from offering gaming in the state without such certification and written approval by the department. The online gaming operator is responsible for all costs associated with testing and obtaining such certifications.

(4) All internet games offered by the online gaming operator shall meet or exceed the technical standards adopted in sections 12-865-15 and 12-865-18 of the Regulations of Connecticut State Agencies and any technical standards established pursuant to section 12-865-3(n) of the Regulations of Connecticut State Agencies. Online gaming operators are prohibited from offering any internet game without written approval by the department. The online gaming operator is responsible for all costs associated with testing and obtaining such approvals.

(aa) Additional electronic wagering platform and internet game technical standards.

(1) Software utilized for gaming shall either:

(A) Continuously display the current time in the state of Connecticut and the time elapsed that a patron has been in the current patron session, or

(B) Cause a pop-up notification, at least every thirty minutes, to be prominently displayed on the remote patron device advising the patron of the current time and the amount of time elapsed since the patron's log on.

(2) An electronic wagering platform shall not induce a patron to continue placing wagers when play is in session, when the patron attempts to stop wagering, when the patron closes the app or program, or when the patron wins or loses a wager.

(3) No auto play feature will be permitted in an electronic wagering platform, unless otherwise provided in subdivision (kk)(6) of this section.

(4) All internet games shall operate in accordance with the game rules and internet gaming account terms and conditions approved by the department.

(bb) Location of servers, security, and cloud storage.

(1) A master wagering licensee and online gaming operator shall place servers or other equipment for the receipt or acceptance of patron wagers and simulcasting live online casino games in secure locations within the state. Equipment not associated with the receipt or acceptance of patron wagers, or simulcasting live online casino games, including remote game servers that are used to determine winners, may be located outside of the state, provided that the location of such equipment complies with all applicable laws, and provided further, that any data located on such equipment shall be available for audit by the department. The location selected shall have adequate security, protections, and controls over the servers or other equipment that is capable of receiving wagers, including those adopted in section 12-865-3(h) of the Regulations of Connecticut State Agencies. The master wagering licensee and online gaming operator shall provide the department with information on the location of all servers and other equipment used in internet gaming under the act, and the department shall have unfettered access to these locations and the data located there with all travel expenses related to inspection of such servers paid for by the master wagering licensee.

(2) The department may approve of the use of cloud storage for duplicate data upon written request of an online gaming operator. All cloud storage shall meet the requirements

of subsection 12-865-3(h) of the Regulations of Connecticut State Agencies.

(cc) Communication standards.

(1) All electronic wagering platforms shall be designed to ensure the integrity and confidentiality of all individual and patron communications and ensure the proper identification of the sender and receiver of all communications.

(2) If communications are performed across a public or third-party network, the electronic wagering platform shall either encrypt the data packets or utilize a secure communications protocol to ensure the integrity and confidentiality of the transmission.

(3) Online gaming operators shall meet or exceed the following communication standards:

(A) Wireless communications between a patron device and an electronic wagering platform that is controlled by the online gaming operator shall be secured using robust wireless security and encryption protocols.

(B) An online gaming operator shall mask the service set identification (SSID) of the electronic wagering platform network to ensure that it is unavailable to the general public.

(C) All communications that contain confidential information, patron data, wagers or results, or patron transaction information shall utilize a secure method of transfer such as:

(i) 256-bit key or higher encryption; or

(ii) any other method approved by the department.

(D) Only devices authorized by the department are permitted to establish communications between a patron device and an electronic wagering platform.

(E) An electronic wagering platform shall maintain an internal clock that reflects the current date and time that shall be used to synchronize the time and date among all components that comprise the electronic wagering platform. The electronic wagering platform date and time shall be visible to a patron when logged on.

(4) All data transfers, including for file integrity check sum verification, shall utilize a minimum of a 256-bit key or higher encryption level.

(5) Notwithstanding the minimum standards established in this section, an online gaming operator shall employ reasonable efforts to ensure it meets or exceeds current industry recognized communication standards, which may include, without limitation, timely replacement or upgrading of obsolete technology.

(dd) Gaming data logging standards.

(1) All electronic wagering platforms shall employ a mechanism capable of maintaining a separate copy of all information the department requires to be logged on a separate and independent logging device capable of being administered by an employee with no incompatible function. For the purposes of this subdivision, "incompatible function" means a function or duties that place any person or department in a position to perpetuate and conceal errors, fraudulent or otherwise. If the electronic wagering platform can be configured such that any logged data is contained in a secure transaction file, a separate logging device is not required.

(2) Online gaming operators shall meet or exceed all gaming data logging standards prescribed by the department and shall address all gaming data logging requirements in the internal controls submitted to the department for approval.

(3) The electronic wagering platform shall provide a mechanism for the department to

query and export, in a read-only format required by the department, all electronic wagering platform data related to internet gaming and retail sport wagering. Data logging standards prescribed by the department are as follows:

(A) Account Creation Log: Electronic wagering platforms shall log the date and time that any account is created or terminated in a secure electronic log.

(B) Internet Gaming Activity Log: Electronic wagering platforms shall maintain all information necessary to recreate a patron's wagering and account activity during each patron session, including any identity or location verifications, for a period of no less than five years in a secure electronic log.

(C) Retail Sports Wagering Activity Log: Electronic wagering platforms shall maintain all information of retail sports wagering conducted at retail sports wagering facilities, for a period of no less than five years in a secure electronic log.

(D) Software Installation and Removal Log: Unless otherwise authorized by the department, when software is installed on or removed from an electronic wagering platform, such action shall be recorded in a secure electronic log. This log shall minimally include the following:

(i) The date and time of the action;

(ii) The identification of the software; and

(iii) The full identity and user ID of the individual performing the action.

(E) Game Availability Log for Internet Casino Gaming: Unless otherwise authorized by the department, when a change in the availability of online casino game software is made on an electronic wagering platform, the change shall be recorded in a secure electronic log including no less than the following:

(i) The date and time of the change;

(ii) The identification of the software; and

(iii) The full identity and user ID of the individual performing the change.

(F) Promotions Log: Unless exempted by the department, an electronic wagering platform shall record all complimentaries and promotions issued and redeemed through the electronic wagering platform in a secure electronic log. This log shall provide the information necessary to audit compliance regarding the terms and conditions of current and previous complimentaries and promotions.

(G) Authentication Log: Results of all authentication attempts shall be retained in a secure electronic log and accessible for no less than a period of ninety days.

(H) Adjustments Log: All adjustments to an electronic wagering platform's data made using stored procedures shall be recorded in a secure electronic log. This log shall contain no less than the following:

(i) The date and time of the adjustment;

(ii) the full identity and user ID of the individual performing the action;

(iii) a description of the event or action taken; and

(iv) the initial and ending values of any data altered as a part of the event or action performed.

(I) If a date and time is required in any log, the following format shall be used:

(i) Date: mm/dd/yyyy; and

(ii) Time: hh:mm:ss.

(ee) Self-monitoring of electronic wagering platform critical components. An electronic wagering platform shall, at least once every twenty-four hours, perform a self-authentication process on all software used to offer, record, and process electronic wagers that is a critical component to ensure there have been no unauthorized modifications. If there is an authentication failure, the electronic wagering platform shall immediately notify the master wagering licensee, the online gaming operator and the department. The results of all self-authentication attempts shall be retained by the electronic wagering platform for not less than ninety days.

(ff) Change approval.

(1) All new core functions shall be tested and certified by a licensed independent testing lab in accordance with this section prior to installation on an electronic wagering platform.

(2) An online gaming operator shall notify the department prior to the installation of any substantial change to a core function on an electronic wagering platform. The notification shall include a clear identification of the core function that is affected, an explanation of the reason for the change, and an identification of any critical files affected.

(3) The department may order that the substantial change to a core function be tested and certified in accordance with this section prior to installation on an electronic wagering platform. If the department does not order testing and certification within seven days after the notification, the online gaming operator may install the substantial change on the electronic wagering platform.

(4) The online gaming operator is not required to notify the department of changes to non-core functions, except when any such change is related to or impacts a core function.

(5) When an unanticipated incident occurs, or is reasonably suspected to have occurred, that causes a disruption in the operation, security, accuracy, integrity, or availability of the electronic wagering system, the online gaming operator shall, upon discovery, notify the department in writing. The online gaming operator may then implement substantial changes to core functions of the electronic wagering platform without prior notification to the department. The online gaming operator a shall submit to the department in writing an incident report that details the incident and the corrections made within twelve hours of such corrective actions. The department may require the online gaming operator to submit the electronic wagering platform to an independent outside lab for recertification and provide the department with the new certification for the electronic wagering platform.

(6) Changes based on subdivision (5) of this subsection shall be documented in the change log and the online gaming operator shall notify the master wagering licensee upon implementation of such changes.

(7) The online gaming operator shall submit change control processes that detail evaluation procedures for all updates and changes to equipment and the electronic wagering platform to the department for approval. These processes shall include details for identifying the criticality of updates and determining the updates that shall be submitted to a licensed independent testing laboratory for review and certification.

(gg) Electronic wagering platform assessment.

(1) Each online gaming operator shall, within ninety days after commencing operations, and annually thereafter, obtain an electronic wagering platform integrity and security assessment conducted by a licensed independent professional selected by the online gaming

operator. The scope of the electronic wagering platform integrity and security assessment is subject to approval of the department and shall include, at a minimum, all of the following:

(A) A vulnerability assessment of internal, external, and wireless networks with the intent of identifying vulnerabilities of all devices, the electronic wagering platform, and applications connected to or present on the networks.

(B) A penetration test of all internal, external, and wireless networks to confirm if identified vulnerabilities of all devices, the electronic wagering platform, and applications are susceptible to compromise.

(C) A policy and procedures review against the current NIST 800 standard or other requirements set forth by the department under section 12-865-3(n) of the Regulations of Connecticut State Agencies.

(D) Any other specific criteria or standards for the electronic wagering platform integrity and security assessment as prescribed by the department.

(2) The independent professional's entire report on the assessment shall be submitted to the department and shall include all the following:

(A) Scope of review;

(B) Name and company affiliation of the individual or individuals who conducted the assessment;

(C) Date of assessment;

(D) Findings;

(E) Recommended corrective action, if applicable; and

(F) Master wagering licensee and online gaming operator's response to the findings and recommended corrective action.

(hh) Online gaming operator's T&S controls.

(1) An online gaming operator shall adopt, implement, and maintain controls that meet or exceed those specified in subdivision (2) of this subsection. The T&S controls shall apply, at a minimum, to all the following critical components of the electronic wagering platform:

(A) Components that record, store, process, share, transmit, or retrieve sensitive information, including, but not limited to, validation numbers, personal identification numbers, and individual and patron data.

(B) Components that generate, transmit, or process random numbers used to determine the outcome of games or virtual events.

(C) Components that store results or the current state of a patron's electronic wager.

(D) Points of entry to and exit from the components provided for in subparagraphs (A) to (C), inclusive, of this subdivision and other systems that are able to communicate directly with core critical electronic wagering platform components.

(E) Communication networks that transmit sensitive information involving internet gaming under the act.

(2) The following T&S controls are the minimum standards an online gaming operator shall incorporate into its internal controls:

(A) T&S controls addressing electronic wagering platform operations and security include, but are not limited to all of the following:

(i) Electronic Wagering Platform Operations and Security. The online gaming operator shall adopt, implement, and maintain procedures for, at a minimum, the following:

(I) Monitoring the critical components and the transmission of data of the entire electronic wagering platform.

(II) Maintenance of all aspects of security of the electronic wagering platform to ensure secure and reliable communications.

(III) Defining, monitoring, documenting, reporting, investigating, responding to, and resolving security incidents.

(IV) Monitoring and adjusting resource consumption and maintaining a log of the electronic wagering platform performance.

(V) Investigating, documenting, and resolving malfunctions.

(ii) Physical Location of Servers and Security. The electronic wagering platform shall be housed in secure locations. Online gaming operators shall provide the department with information on the location of all electronic wagering platform servers. The secure locations shall have sufficient protection from unauthorized access and physical and environmental hazards and be equipped with surveillance and security systems that meet or exceed industry standards.

(iii) Electronic Wagering Platform Logical Access Controls. The electronic wagering platform shall be logically secured against unauthorized access.

(iv) Electronic Wagering Platform User Authorization. The electronic wagering platform shall be subject to user authorization requirements as required by the department.

(v) Server Programming. The electronic wagering platform shall be sufficiently secure to prevent any user-initiated programming capabilities on the server that may result in unauthorized modifications to the database.

(vi) Verification Procedures. Procedures shall be in place for verifying on demand that the critical control program components of the electronic wagering platform in the production environment are identical to those approved by the department.

(vii) Electronic Document Retention System. The online gaming operator shall establish procedures that ensure that all reports required under the act and sections 12-865-1 to 12-865-34, inclusive, of the Regulations of Connecticut State Agencies are stored in an electronic document retention system.

(viii) Asset Management. All assets that house, process, or communicate sensitive information, including those comprising the operating environment of the electronic wagering platform or its components, or both, shall be accounted for and have a key employee that is responsible for each asset.

(B) T&S controls addressing data security and backup recovery include, but are not limited to, all of the following:

(i) Data Security. The electronic wagering platform shall provide a logical means for securing individual and patron data and wagering data, including accounting, reporting, significant event, or other sensitive information, against alteration, tampering, or unauthorized access.

(ii) Data Alteration. The alteration of any accounting, reporting, or significant event data relating to electronic wagering under the act is not permitted without supervised access controls. If any data is changed, all information required by the department shall be documented or logged.

(iii) Backup Frequency. Backup scheme implementation relating to information

involving electronic wagering under the act shall occur at least once every day or as otherwise specified by the department.

(iv) Storage Medium Backup. Audit logs, electronic wagering platform databases, and any other pertinent patron data and wagering data shall be stored using reasonable protection methods. The electronic wagering platform shall be designed to protect the integrity of this data if there is a failure. Redundant copies of this data shall be kept on the electronic wagering platform with open support for backups and restoration, so that no single failure of any portion of the electronic wagering platform would cause the loss or corruption of the data.

(v) Electronic Wagering Platform Failure. The electronic wagering platform shall have sufficient redundancy and modularity so that if any single component or part of a component fails, the functions of the electronic wagering platform and the process of auditing those functions can continue with no critical data loss. If two or more components are linked, the process of all electronic wagering operations between the components shall not be adversely affected by restart or recovery of either component and upon restart or recovery, the components shall immediately synchronize the status of all transactions, data, and configurations with one another.

(vi) Accounting and Master Resets. The online gaming operator shall be able to identify and properly handle the situation where a master reset has occurred on any component that affects gaming under the act.

(vii) Recovery Requirements. If there is a catastrophic failure which results in the electronic wagering platform being unable to be restarted in any other way, the electronic wagering platform shall be restored from the last backup point and fully recovered. The contents of that backup shall contain all critical information to fully restore the electronic wagering platform as required by the department.

(viii) Uninterrupted Power Supply (UPS) Support. All electronic wagering platform components shall be provided with adequate primary power. If the server is a stand-alone application, it shall have a UPS connected and shall have sufficient capacity to permit a methodical shut-down that retains all individual and patron data and wagering data during a power loss. It is acceptable that the electronic wagering platform may be a component of a network that is supported by a network-wide UPS if the server is included as a device protected by the UPS. There shall be a surge protection system in use if not incorporated into the UPS itself.

(ix) Business Continuity and Disaster Recovery Plan. A business continuity and disaster recovery plan shall be in place to recover gaming and wagering operations if the electronic wagering platform's production environment is rendered inoperable.

(C) T&S controls addressing communications include, but are not limited to, all of the following:

(i) Connectivity. Only authorized devices are permitted to establish communications between any electronic wagering platform components.

(ii) Communication Protocol. Each component of the electronic wagering platform shall function as indicated by a documented secure communication protocol.

(iii) Communication Over Electronic and Public Networks. Communications between electronic wagering platform components shall be secure. Patron data, confidential

information, wagers, results, financial information, and patron transaction information related to gaming shall always be encrypted and protected from incomplete transmissions, misrouting, unauthorized message modification, disclosure, duplication, or replay.

(iv) Wireless Local Area Network Communications. The use of wireless local area network communications shall adhere to applicable requirements specified for wireless devices and is subject to approval by the department.

(v) Network Security Management. Networks shall be logically separated to ensure that there is no network traffic on a network link that cannot be serviced by hosts on that link.

(vi) Mobile Computing and Communications. Formal policies shall be in place, and appropriate security measures shall be adopted to protect against the risk of using mobile computing and communication facilities. Telecommuting shall not be permitted except under circumstances where the security of the endpoint can be guaranteed.

(D) T&S controls addressing third party service providers include, but are not limited to, communications between the electronic wagering platform and third-party service providers. Where communications related to internet gaming are implemented with third-party service providers, the electronic wagering platform shall securely communicate with all third-party service providers utilizing encryption and strong authentication, ensure that all login events are recorded to an audit file, and ensure that all communications do not interfere or degrade normal electronic wagering platform functions.

(E) T&S controls addressing information security, include but are not limited to, all of the following:

(i) Domain Name Service Requirements. The online gaming operator shall establish requirements that apply to servers used to resolve domain name service queries used in association with the electronic wagering platform.

(ii) Cryptographic Controls. The online gaming operator shall establish and implement a policy for the use of cryptographic controls that ensures the protection of information.

(iii) Encryption Key Management. The management of encryption keys shall follow defined processes established by the online gaming operator.

(F) The T&S controls addressing remote access and firewalls include, but are not limited to, all of the following:

(i) Remote Access Security. Remote access, if approved by the department, shall be performed via a secured method, shall have the option to be disabled, may accept only the remote connections permissible by the firewall application and electronic wagering platform settings, and shall be limited to only the application functions necessary for users to perform their job duties.

(ii) Remote Access and Test Account Procedures. Remote access and test account procedures shall be established that ensure that remote access is strictly controlled.

(iii) Remote Access Activity Log. The remote access application shall maintain an activity log that updates automatically and records and maintains all remote access information.

(iv) Firewalls. All communications, including remote access, shall pass through at least one approved application-level firewall. This includes connections to and from any non-electronic wagering platform hosts used by the online gaming operator.

(v) Firewall Audit Logs. The firewall application shall maintain an audit log and shall

disable all communications and generate an error if the audit log becomes full. The audit log shall contain, at a minimum, all the following information:

(I) All changes to configuration of the firewall.

(II) All successful and unsuccessful connection attempts through the firewall.

(III) The source and destination IP addresses, port numbers, protocols, and, where possible, MAC addresses.

(vi) Firewall Rules Review. The firewall rules shall be reviewed no less than twice each calendar year by the master wagering licensee and online gaming operator to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets. The review shall be performed on all the perimeter firewalls and the internal firewalls.

(G) T&S controls addressing change management include, but are not limited to, all of the following:

(i) Program Change Control Procedures. Program change control procedures shall ensure that only authorized versions of programs are implemented on the production environment.

(ii) Software Development Life Cycle. The acquisition and development of new software shall follow defined processes established by the master wagering licensee, online gaming operator or online gaming service provider and subject to review by the department.

(iii) Patches. All patches should be tested, as applicable, in a development and test environment configured to match the target production environment before being deployed into production. Permitted exceptions and related procedures and controls shall be fully addressed.

(H) T&S controls addressing periodic security testing include, but are not limited to, all of the following:

(i) Technical Security Testing. Periodic technical security tests on the production environment shall be performed quarterly or as required by the department to guarantee that no vulnerabilities putting at risk the security and operation of the electronic wagering platform exist.

(ii) Vulnerability Assessment. The online gaming operator shall conduct vulnerability assessments. The purpose of the vulnerability assessment is to identify vulnerabilities, which could be later exploited during penetration testing by making basic queries relating to services running on the electronic wagering platform concerned.

(iii) Penetration Testing. The online gaming operator shall conduct penetration testing. The purpose of the penetration testing is to exploit any weaknesses uncovered during the vulnerability assessment on any publicly exposed applications or electronic wagering platform hosting applications processing, transmitting, or storing sensitive information.

(iv) Information Security Management System (ISMS) Audit. An audit of the ISMS will be periodically conducted, including all the locations where sensitive information is accessed, processed, transmitted, or stored. The ISMS will be reviewed against common information security principles in relation to confidentiality, integrity, and availability such as NIST 800 or other requirements set forth by the department under Section 12-865-3(n) of the Regulations of Connecticut State Agencies.

(v) Cloud Service Audit. An online gaming operator that utilizes a cloud service provider (CSP), if approved by the department, to store, transmit, or process sensitive information

shall undergo a specific audit as required by the department. The CSP shall be reviewed against common information security principles in relation to the provision and use of cloud services, such as NIST 800, or other requirements set forth by the department under section 12-865-3(n) of the Regulations of Connecticut State Agencies.

(3) The online gaming operator shall include the T&S controls in the operator's internal controls and electronic wagering platform submitted to the department for approval.

(4) The T&S controls shall:

(A) Have a provision requiring review when changes occur to the electronic wagering platform;

(B) Be approved by the online gaming operator's senior management;

(C) Be communicated to all affected employees and relevant external parties;

(D) Undergo review at planned intervals; and

(E) Delineate the responsibilities of the master wagering licensee's staff, the online gaming operator's staff, and the staff of any third parties for the operation, service, and maintenance of the electronic wagering platform or its components, or both.

(ii) An online gaming operator or online gaming service provider may establish test accounts to be used to test the various components and operation of an electronic wagering platform pursuant to internal controls adopted by the online gaming operator, which, at a minimum, shall address all of the following:

(1) The procedures for issuing funds used for testing, including the identification of who may issue the funds and the maximum amount of funds that may be issued.

(2) The procedures for assigning each test account for use by only one individual. However, an online gaming operator may establish a specific scenario or instance of a test account that may be shared by multiple users if each user's activities are separately logged.

(3) The maintenance of a record for all test accounts, to include when the test account is active, to whom the test account is issued, and the employer of the individual to whom the test account is issued.

(4) The procedures for auditing testing activity by the online gaming operator or online gaming service provider to ensure the accountability of funds used for testing and proper adjustments to gross gaming revenue from internet games and retail sports wagering.

(5) The procedures for authorizing and auditing out-of-state test activity.

(jj) The online gaming operator shall put in place procedures to permit the department to establish test accounts on the electronic wagering platform.

(kk) Electronic wagering platforms shall include the following patron protections:

(1) The electronic wagering platform shall not force game play as follows:

(A) The patron may not be forced to play an internet game just by selecting that game.

(B) It shall not be possible to start a new internet game in the same patron user session before all relevant account balances have been updated on the electronic wagering platform.

(2) Bots are only permitted when employed by the electronic wagering platform in free play or training mode, or if use of the bot satisfies all of the following:

(A) The use of artificial intelligence software is clearly explained in the help menus and game rules; and

(B) All bots engaging in internet gaming shall be clearly marked so that patrons are aware of which players are not human.

(3) Patrons shall be prohibited from utilizing bots, automated computerized software or other equivalent mechanism to engage in play.

(4) No patron shall occupy more than one position at an online casino game at any given time, unless such conduct is authorized in advance by the department for a specific casino game.

(5) A game is incomplete when the internet game outcome remains unresolved or the outcome cannot be properly seen by the patron.

(A) The online gaming operator may provide a mechanism for a patron to complete an incomplete internet game.

(B) Incomplete internet games shall be resolved before a patron is permitted to participate in another instance of the same game.

(C) Wagers associated with an incomplete game shall be voided, and recorded in the change log required pursuant to section 12-865-34 of the Regulations of Connecticut State Agencies, and the wagers can be forfeited or returned to the patron provided that:

(i) The terms and conditions or the game rules, or both, shall clearly define how wagers will be handled when they remain undecided beyond the specified time period and the electronic wagering platform shall be capable of returning or forfeiting the wagers, as appropriate.

(ii) In the event that a game cannot be continued due to an electronic wagering platform action, all wagers shall be returned to the patrons playing that game, except that if a patron's participation in the game prior to its discontinuance was such that the patron would have received winnings greater than the wager, the patron shall be provided the amount of winnings earned prior to discontinuance in addition to the return of the wager.

(6) Auto play of internet games shall be prohibited. Internet game play shall be initiated only after a patron has affirmatively placed a wager and activated play. An auto play feature is not permitted in interactive online game software unless the department determines that the auto play feature will not cause substantial financial harm to patrons, nor a security or gaming integrity concern for the department, and the department provides written approval of such feature. If an auto play feature is authorized by the department, it shall be possible for a patron to turn auto play off at any time during game play.

(Effective February 1, 2022)