

Sec. 12-865-32. Data Privacy Provisions

(a) Gaming entity licensees shall provide a readily accessible privacy policy to patrons on its electronic wagering platform. The privacy policy shall state the information that is required to be collected, the purpose for information collection, and the conditions under which information may be disclosed. Any information about a patron's internet gaming account that is not subject to disclosure pursuant to the privacy policy shall be kept confidential, except where the release is required by law or requested by the department. Patron information shall be securely erased from all storage media, including but not limited to HDD, SSD, Flash, Mobile, Cloud, Virtual, RAID, LUN, hard disks, solid state memory, and other devices before the device is decommissioned. If erasure is not possible, the storage device shall be destroyed.

(b) Gaming entity licensees shall take reasonable steps to ensure that confidential information security measures are implemented which, at a minimum, shall:

(1) Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of confidential information and to ensure secure and timely disposal of such information once there is no longer a business need for such information;

(2) Create a data minimization plan to ensure that only data required to ensure the verification of a patron's identity and authenticate patron financial information is collected. Such plan shall also set forth the licensee's policy for data destruction after the applicable record retention expiration date;

(3) Immediately, but in no event later than one business day, notify the department after becoming aware of a suspected confidential information breach;

(4) Within five business days of notifying the department of a suspected confidential information breach, provide the department a written notice that (A) details the suspected or confirmed confidential information breach, including the licensee's plan to remediate the breach, mitigate its effects, and prevent breaches of a similar nature from occurring in the future, or (B) details why, upon further investigation, the licensee believes that a breach did not occur;

(5) Upon request of the department, provide a forensic report from a qualified third-party forensic examiner, the cost of which report shall be paid by the licensee contracting for the report;

(6) Establish and publish privacy protection policies on the gaming entity licensee's website that shall include, but not be limited to: safeguarding confidential information, computer files and documents containing confidential information from misuse by third parties; and destroying, erasing or making unreadable such confidential information, computer files and documents prior to disposal; and

(7) Comply with the breach of security reporting requirements of section 36a-701b of the Connecticut General Statutes.

(c) Every written agreement that authorizes a master wagering licensee or online gaming operator to share confidential information with an online gaming service provider or sports wagering retailer shall require the online gaming service provider or sports wagering retailer to do the following:

(1) At its own expense, protect any and all confidential information that it comes to

possess or control, wherever and however stored or maintained, against a confidential information breach;

(2) Implement and maintain a comprehensive data-security program for the protection of confidential information. The safeguards contained in such program shall be consistent with and comply with the safeguards for protection of confidential information as set forth in all applicable federal and state law. Such data-security program shall include, but not be limited to, the following: (A) A security policy for employees related to the storage, access and transportation of data containing confidential information; (B) reasonable restrictions on access to records containing confidential information, including the area where such records are kept and secure passwords for electronically stored records; (C) a process for reviewing policies and security measures at least annually; and (D) an active and ongoing employee security awareness program that is mandatory for all employees who may have access to confidential information associated with Connecticut internet gaming or sports wagering that, at a minimum, advises such employees of the confidentiality of the information, the safeguards required to protect the information and any applicable civil and criminal penalties for noncompliance pursuant to state and federal law;

(3) Limit access to confidential information to authorized employees and authorized agents of the gaming entity licensee, for authorized purposes as necessary for the business operations of the licensee;

(4) Maintain all electronic data constituting confidential information obtained pursuant to activity authorized by the act: (A) In a secure server; (B) on secure drives; (C) behind firewall protections and monitored by intrusion detection software; (D) in a manner where access is restricted to employees and agents authorized by the online gaming service provider or sports wagering retailer; and (E) as otherwise required under state and federal law;

(5) Implement, maintain and update security and breach investigation and incident response procedures that are appropriate given the nature of the information involved and that are reasonably designed to protect confidential information from unauthorized access, use, modification, disclosure, manipulation or destruction; and

(6) Include a provision in any agreement the online gaming service provider or sports wagering retailer enters into with a third-party provider or anyone with access to the confidential information, that such provider or person shall comply with the provisions of subsections (b)(1) to (b)(6), inclusive, of this section.

(d) Master wagering licensees, online gaming operators, online gaming service providers and sports wagering retailers shall prohibit unauthorized persons from accessing proprietary internet game programming and electronic wagering platform information. In the event that a gaming entity licensee or key employee of such gaming entity licensee becomes aware of a compromise or potential compromise of security regarding exposure of proprietary internet game or electronic wagering platform information that could impact the integrity of gaming or gross gaming revenue, the gaming entity licensee or key employee shall notify the department within one business day of discovery of such concern. The gaming entity licensee shall thereafter take all necessary steps to restore security as quickly as possible, including submitting a report detailing either (1) the occurrence of the breach or suspected breach, including a plan to mitigate the effects of any breach and specifying the steps taken

to ensure future breaches do not occur, or (2) why, upon further investigation, the licensee believes no breach has occurred.

(e) Online gaming service providers shall be prohibited from retaining patron internet account information without the expressed written consent of the online gaming operator or master wagering licensee.

(f) Online gaming service providers and online gaming operators shall obtain a patron's consent, which may be withdrawn at any time, for the online gaming service provider or online gaming operator to transmit, collect, maintain, process and use the patron's location data for any purpose beyond verifying the location of a patron for purposes of complying with the act and sections 12-865-1 to 12-865-34, inclusive, of the Regulations of Connecticut State Agencies. Online gaming service providers and online gaming operators shall request a patron's consent prior to utilizing or transmitting the patron's personally identifiable information, individual gaming information or location data for any purpose other than complying with geolocation restrictions under the act and sections 12-865-1 to 12-865-34, inclusive, of the Regulations of Connecticut State Agencies. If the patron turns off the location settings on the patron device such that the online gaming service provider cannot verify the patron's location for purposes of complying with the act or sections 12-865-1 to 12-865-34, inclusive, of the Regulations of Connecticut State Agencies, the patron shall not be able to place wagers. If a patron's location shall be verified through the patron's browser location services, the patron shall give the patron's consent for such verification, which shall be obtained through an interactive message that appears when the patron tries to make a wager.

(g) Information relating to a patron's location and the location of the patron's device shall be shared with the department upon request. Records confirming a patron's location may be retained by the department for auditing purposes.

(h) The department may request information from licensees that includes personal information of the licensee, patrons or occupational employees. The department shall only request personal information that is necessary in order for it to carry out its functions. Gaming entity licensees shall ensure that their privacy notices advise patrons that their personal information may be shared with the department.

(Effective February 1, 2022)