CHAPTER 809a. INTERACTIVE GAMING PLATFORM REQUIREMENTS

Sec.

Authority

The provisions of this Chapter 809a added under 4 Pa.C.S. §§ 1202(b)(30) and 13B02, unless otherwise noted.

Source

The provisions of this Chapter 809a added August 27, 2021, effective August 28, 2021, 51 Pa.B. 5389, unless noted otherwise.

Cross References

This section cited in 58 Pa. Code § 830a.7 (relating to multiuse computing device and gaming platform requirements); 58 Pa. Code § 1401a.1 (relating to scope); and 58 Pa. Code § 1407a.8 (relating to sports wagering interactive system requirements).

§ 809a.1. Scope.

To ensure players are not exposed to unnecessary security risks by choosing to participate in interactive gaming in this Commonwealth and to ensure the integrity and security of interactive gaming operations in this Commonwealth, the system requirements in this chapter apply to all of the following critical components of an interactive gaming system:

(1) Interactive gaming system components which record, store, process, share, transmit or retrieve sensitive player information (for example, credit and debit card details, authentication information and player account balances).

(2) Interactive gaming system components which generate, transmit or process random numbers used to determine the outcome of games or virtual events.

(3) Interactive gaming system components which store results or the current state of a player's wager.

(4) Points of entry and exit from the previously listed systems or other systems which are able to communicate directly with core critical systems.

(5) Communication networks which transmit sensitive player information.

§ 809a.2. Definitions.

The following words and terms, when used in this chapter, have the following meanings, unless the context clearly indicates otherwise:

Domain name system—The globally distributed Internet database which maps machine names to IP numbers, and vice versa.

Player device—The device that converts communications from the interactive gaming platform into a human interpretable form and converts human decisions into a communication format understood by the interactive gaming platform. The term includes personal computers, mobile phones, tablets, and the like.

Primary server—First source for Domain Name System data and responses to queries.

Remote access—Any access from outside the interactive gaming system or interactive gaming system network, including access from other networks within the same facility.

Secondary server or *redundancy server*—A server that shares the same features and capabilities as the primary server serves and acts as a second or substitutive point of contact in case the primary server is unavailable, busy or overloaded.

Stateful protocol—A protocol in which the communication system utilized by the player and the primary or secondary server tracks the state of the communication session.

Stateless protocol—A protocol in which neither the player nor the primary or secondary servers communication systems tracks the state of the communication session.

§ 809a.3. Location of equipment.

(a) The Board shall approve the location of all interactive gaming devices and associated equipment used by an interactive gaming certificate holder or interactive gaming operator to conduct interactive gaming. The interactive gaming devices and associated equipment may be located in a restricted area on the premises of the licensed facility, in an interactive gaming restricted area within the geographic limits of the county in this Commonwealth where the licensed facility is situated or any other area, located within the United States, provided the location adheres to all of the following limitations:

(1) The primary server used to resolve domain name service inquiries used by an interactive gaming certificate holder or interactive gaming operator to conduct interactive gaming in this Commonwealth must be physically located in a secure data center.

(2) Any redundancy, secondary and emergency servers used by an interactive gaming certificate holder or interactive gaming operator to conduct interactive gaming in this Commonwealth must be physically located in a secure data center at a separate premises than the primary server within the Commonwealth.

(b) The Board may require interactive gaming system data necessary to certify revenue and resolve player complaints to be maintained in this Common-

wealth in a manner and location approved by the Board. The data must include data related to the calculation of revenue, player transactions, game transactions, game outcomes, responsible gaming and any other data which may be prescribed by the Board. The data must be maintained in a manner which prevents unauthorized access or modification without the prior approval of the Board.

§ 809a.4. Physical and environmental controls for equipment.

(a) An interactive gaming system and the associated communications systems must be located in facilities which provide physical protection against damage from fire, flood, hurricane, earthquake, and other forms of natural or manmade disaster by utilizing and implementing at least all of the following measures:

(1) Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) must be used to protect areas that contain interactive gaming systems components.

(2) Secure areas must be protected by appropriate entry controls to ensure that access is restricted to only authorized personnel.

(3) All access must be recorded in a secure log which is available for inspection by Board staff.

(4) Secure areas must include an intrusion detection system. Attempts at unauthorized access must be logged.

(b) Interactive gaming system servers must be located in server rooms which prohibit unauthorized access.

(c) Interactive gaming system servers must be housed in racks located within a secure area.

(d) Interactive gaming system components must provide all of the following minimum utility support:

(1) Interactive gaming system components must be provided with adequate primary power.

(2) Interactive gaming system components must have uninterruptible power supply equipment to support operations in the event of a power failure.

(3) There must be adequate cooling for the equipment housed in the server area.

(4) Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.

(5) There must be adequate fire protection for the interactive gaming system components housed in the server room.

§ 809a.5. Access to equipment.

(a) The interactive gaming certificate holder and interactive gaming operator shall limit and control access to the primary server and any secondary servers by ensuring all of the following:

(1) Maintain access codes and other computer security controls.

(2) Maintain logs of user access, security incidents and unusual transactions.

(3) Coordinate and develop an education and training program on information security and privacy matters for employees and other authorized users.

(4) Ensure compliance with all State and Federal information security policies and rules.

(5) Prepare and maintain security-related reports and data.

(6) Develop and implement an incident reporting and response system to address security breaches, policy violations and complaints from external parties.

(7) Develop and implement an ongoing risk assessment program that targets information security and privacy matters by identifying methods for vulnerability detection and remediation and overseeing the testing of those methods.

(b) Remote access to an interactive gaming certificate holder or interactive gaming operator's interactive gaming system is only permitted as follows:

(1) To Board employees upon request and without limitation.

(2) For testing purposes with prior approval from and as limited by the Board.

(3) By employees of an interactive gaming certificate holder or an interactive gaming operator with prior approval from and as limited by the Board.

(c) All interactive gaming certificate holder's or interactive gaming operator's interactive gaming systems must be available for independent testing by the Board, without limitation.

§ 809a.6. System requirements.

(a) *Interactive gaming system methodology*. An interactive gaming system shall be designed with a methodology (for example, cryptographic controls) approved by the Board to ensure secure communications between a player's device and the interactive gaming system. When reviewing the security of an interactive gaming certificate holder or interactive gaming operator's interactive gaming system methodology, the Board will consider all of the following:

(1) The interactive gaming system methodology shall be designed to ensure the integrity and confidentiality of all player communication and ensure the proper identification of the sender and receiver of all communications. If communications are performed across a third-party network, the system must either encrypt the data packets or utilize a secure communications protocol to ensure the integrity and confidentiality of the transmission.

(2) Wireless communications between the player device and the primary or secondary server must be encrypted in transit using a method (for example, AES, IPsec and WPA2) approved by the Board.

(3) All communications that contain registered player account numbers, user identification, or passwords and PINs must utilize a secure method of transfer (for example, 128-bit key encryption) approved by the Board.

(4) Only devices authorized by the Board are permitted to establish communications between a player device and an interactive gaming system.

(5) Server-based interactive gaming systems must maintain an internal clock that reflects the current date and time that must be used to synchronize the time and date among all components that comprise the interactive gaming system. The interactive gaming system date and time must be visible to the registered player when logged on.

(b) *Change or modification*. Any change or modification to the interactive gaming system shall be handled in accordance with the Change Management guidelines issued and distributed to interactive gaming certificate holders, interactive gaming operators, and interactive gaming manufacturers.

(c) *Standards for data logging*. An interactive gaming system must meet all of the following standards regarding data logging:

(1) Interactive gaming systems must employ a mechanism capable of maintaining a separate copy of all of the information required to be logged in this section on a separate and independent logging device capable of being administered by an employee with no incompatible function. If the interactive gaming system can be configured so that any logged data is contained in a secure transaction file, a separate logging device is not required.

(2) Interactive gaming systems must provide a mechanism for the Board to query and export, in a format required by the Board, all interactive gaming system data.

(3) Interactive gaming systems must electronically log the date and time any player gaming account is created or terminated (Account Creation Log).

(4) An interactive gaming system must maintain all information necessary to recreate player game play and account activity during each player session, including any identity or location verifications, for not less than 10 years.

(5) Unless otherwise authorized by the Board, when software is installed on or removed from an interactive gaming system, the action must be recorded in a secure electronic log (Software Installation/Removal Log), which must include all of the following:

(i) The date and time of the action.

(ii) The identification of the software.

(iii) The identity of the person performing the action.

(6) Unless otherwise authorized by the Board, when a change in the availability of game software is made on an interactive gaming system, the change must be recorded in a secure electronic log (Game Availability Log), which must include:

(i) The date and time of the change.

(ii) The identification of the software.

(iii) The identity of the person performing the change.

(7) Unless otherwise exempted by the Board, an interactive gaming system must record all promotional offers (Promotions Log) issued through the system. The log must provide the information necessary as determined by the Board to audit compliance with the terms and conditions of current and previous offers.

(8) Results of all authentication attempts must be retained in an electronic log (Authentication Log) and accessible for not less than 90 days.

(9) All adjustments to an interactive gaming system data made using stored procedures must be recorded in an electronic log (Adjustments Log), which lists all of the following:

(i) The date and time.

(ii) The identification and user ID of user performing the action.

(iii) A description of the event or action taken.

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

(d) *Security requirements*.

(1) Networks should be logically separated so that there should be no network traffic on a network link which cannot be serviced by hosts on that link.

(2) Networks must meet all of the following requirements to assure security:

(i) The failure of any single item should not result in a denial of service.

(ii) An intrusion detection system/intrusion prevention system must be installed on the network which can do all of the following:

(A) Listen to both internal and external communications.

(B) Detect or prevent Distributed Denial of Service attacks.

(C) Detect or prevent shellcode from traversing the network.

(D) Detect or prevent Address Resolution Protocol spoofing.

(E) Detect other Man-in-the-Middle indicators and server communication immediately.

(iii) Each server instance in cloud and virtualized environments should perform only one function.

(iv) In virtualized environments, redundant server instances cannot run under the same hypervisor.

(v) Stateless protocols should not be used for sensitive data without stateful transport.

(vi) All changes to network infrastructure must be logged.

(vii) Virus scanners or detection programs, or both, should be installed on all pertinent information systems and should be updated regularly to scan for new strains of viruses.

(viii) Network security should be tested by a qualified and experienced individual on a regular basis.

(ix) Testing should include testing of the external interfaces and internal network.

(x) Testing of each security domain on the internal network should be undertaken separately.

(3) An annual security audit shall be performed to complement the required independent testing laboratory testing and annual encryption certification.

(i) The security audit shall cover the underlying operating systems, network components and hardware changes not included in the evaluation of the interactive gaming software.

(ii) The security audit shall be performed by an independent third party who shall provide a detailed report with remediation or mitigation plans to the board, and may take the form of any of the following:

(A) Penetration test.

(B) Vulnerability assessment.

(C) Compliance audit.

(D) Risk assessment.

(4) Internal and external network vulnerability scans shall be run at least quarterly, or after any change or modification to the interactive gaming system that requires approval by the Board under the change management guidelines distributed under § 809a.6(b) (relating to system requirements), unless otherwise directed by the Board.

(i) Testing procedures must verify that four quarterly internal and external scans take place every 12 months and that re-scans occur until all medium risk (CVSS4.0 or higher) vulnerabilities are resolved.

(ii) The quarterly scans may be performed by either an independent third party or by a qualified employee of the interactive gaming certificate holder or interactive gaming operator.

(iii) Verification of the scans shall be submitted to the Board on a quarterly basis and must include a remediation or mitigation plan for any vulnerabilities not resolved prior to the submission of the verification.

(e) *Self-monitoring of critical components*. The interactive gaming system must implement the self-monitoring of critical components. A critical component that fails self-monitoring tests shall be taken out of service immediately and may not be returned to service until there is reasonable evidence that the fault has been rectified. Required self-monitoring measures include all of the following:

(1) The clocks of all components of the interactive gaming system must be synchronized with an agreed accurate time source to ensure consistent logging. Time skew shall be checked periodically.

(2) Audit logs recording user activities, exceptions and information security events must be produced and kept for a period of time to be determined by the Board to assist in investigations and access control monitoring.

(3) System administrators and system operator activities must be logged.

(4) Logging facilities and log information must be protected against tampering and unauthorized access.

(5) Any modifications, attempted modifications, read access, or other change or access to any interactive gaming system record, audit or log must be detectable by the interactive gaming system. It must be possible to see who has viewed or altered a log and when.

(6) Logs generated by monitoring activities shall be reviewed periodically using a documented process. A record of each review must be maintained.

(7) Interactive gaming system faults shall be logged, analyzed and appropriate actions taken.

(8) Network appliances with limited onboard storage must disable all communication if the audit log becomes full or offload logs to a dedicated log server.

(f) *System disclosure requirements.*

(1) A petitioner for or holder of an interactive gaming certificate, an applicant for or holder of an interactive gaming license, and an applicant for or holder of an interactive gaming manufacturer license shall seek Board approval of all source code used to conduct interactive gaming in this Commonwealth.

(2) All documentation relating to software and application development should be available for Board inspection and retained for the duration of its lifecycle.

(3) All software used to conduct interactive gaming in this Commonwealth shall be designed with a method, approved by the Board, that permits remote validation of software.

(g) *Shutdown and recovery capabilities*. The interactive gaming system must have all of the following shutdown and recovery capabilities to maintain the integrity of the hardware, software and data contained therein in the event of a shutdown:

(1) The interactive gaming system must be able to perform a graceful shutdown and only allow automatic restart on power up after all of the following procedures have been performed:

(i) The program resumption routine, including self-tests, completes successfully.

(ii) All critical control program components of the interactive gaming system have been authenticated using a method approved by the Board.

(iii) Communication with all components necessary for the interactive gaming system operation have been established and similarly authenticated.

(2) The interactive gaming system must be able to identify and properly handle the situation when master resets have occurred on other remote gaming components which affect game outcome, win amount or reporting.

(3) The interactive gaming system must have the ability to restore the system from the last backup.

(4) The interactive gaming system must be able to recover all critical information from the time of the last backup to the point in time at which the interactive gaming system failure or reset occurred.

(h) *Recovery plan*. An interactive gaming certificate holder or interactive gaming operator shall have a plan in place, approved by the Board, to recover interactive gaming operations in the event that the interactive gaming system is rendered inoperable (that is, Disaster/Emergency Recovery Plan). When reviewing the sufficiency of an interactive gaming certificate holder or interactive gaming operator's plan to recover interactive gaming system operations in the event the interactive gaming system is rendered inoperable, the Board will consider all of the following:

(1) The method of storing player account information and gaming data to minimize loss in the event the interactive gaming system is rendered inoperable.

(2) If asynchronous replication is used, the method for recovering data should be described or the potential loss of data should be documented.

(i) *Recovery plan requirements*. An interactive gaming certificate holder's or interactive gaming operator's Disaster/Emergency Recovery Plan must also:

(1) Delineate the circumstances under which it will be invoked.

(2) Address the establishment of a recovery site physically separated from the interactive gaming system site.

(3) Contain recovery guides detailing the technical steps required to re-establish gaming functionality at the recovery site.

(4) Include a Business Continuity Plan that addresses the process required to resume administrative operations of interactive gaming activities after the activation of the recovered platform for a range of scenarios appropriate for the operations context of the interactive gaming system.

(j) *Location of equipment*. Equipment used by a server-based interactive gaming system for the sole purpose of restoring data following a disaster must be located in a location within the United States as approved by the Board.

(k) *Player self-exclusion*. The interactive gaming system must provide an easy and obvious mechanism for players to access the Board's self-exclusion database to self-exclude from interactive gaming.

(l) *Mechanism for temporary suspension*. The interactive gaming system must provide a mechanism by which a player may elect to temporarily suspend his or her interactive gaming account for a period of no less than 72 hours in accordance with the terms and conditions agreed to by the player upon registration.

Cross References

This section cited in 58 Pa. Code § 809a.6 (relating to system requirements).

§ 809a.7. Geolocation requirements.

(a) An interactive gaming system must employ a mechanism to detect the physical location of a player upon logging into the interactive gaming system and as frequently as specified in the Board's technical standards and the interactive gaming certificate holder's or interactive gaming operator's approved internal

controls submission. If the system detects that the physical location of the player is in an area unauthorized for an interactive gaming system, the system shall not accept wagers and must disable any interactive gaming activity for that player until the player is in an authorized location.

(b) The geolocation system must be equipped to dynamically monitor the player's location and block unauthorized attempts to access the interactive gaming system throughout the duration of the gaming session.

(c) An interactive gaming certificate holder or interactive gaming operator must prevent registered players within a licensed facility from accessing authorized interactive games on the registered player's own computers or other devices through the use of geolocation technologies.

(d) Interactive gaming shall only occur within this Commonwealth unless the conduct of gaming is not inconsistent with Federal law, law of the jurisdiction, including any foreign nation, in which the participating player is located, or the gaming activity is conducted pursuant to a reciprocal agreement to which the Commonwealth is a party that is not inconsistent with Federal law.

Cross References

This section cited in 58 Pa. Code § 830a.7 (relating to multiuse computing device and gaming platform requirements).

§ 809a.8. Security policy requirements.

Interactive gaming certificate holders and interactive gaming operators shall adopt and maintain a Board-approved information security policy which describes the certificate holder's or licensee's approach to managing information security and its implementation. This policy is required in addition to any similar requirements that may be imposed as part of the certificate holder's or licensee's internal controls. The information security policy must:

(1) Conform to the standards of the most recent version of the NIST cybersecurity framework.

(2) Be reviewed annually as well as when significant changes occur to the interactive gaming system or the processes which alter the risk profile of the interactive gaming system.

(3) Be approved annually by the certificate holder's or operator's management.

(4) Be communicated to all employees and relevant external parties.

(5) Delineate the responsibilities of the certificate- holder's or licensee's staff and the staff of any third parties for the operation, service and maintenance of the interactive gaming system and its components.

[Next page is 810-1.]