Subpart L. Interactive Gaming – Temporary Regulations

Chapter 809. INTERACTIVE GAMING PLATFORM REQUIRMENTS – TEMPOARY REGULATIONS

Sec.

§ 809.1. 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 the following critical components of an interactive gaming system:

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

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

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

(d) Points of entry and exit from the above systems (other systems which are able to communicate directly with core critical systems).

(e) Communication networks which transmit sensitive player information.

§ **809.1. 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.

Primary server - First source for Domain Name System (DNS) data and responds to queries.

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

Remote access – Any access from outside the interactive gaming system or interactive gaming system network, including any 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 track the state of the communication session.

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

§ **809.3. Location of equipment.**

The Board shall approve the location of all interactive gaming devices and associated equipment used by an interactive gaming certificateholder or interactive gaming licensee to conduct interactive gaming. The 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 the following limitations:

(a) The primary server used to resolve "domain name service" ("DNS") inquiries used by an interactive gaming certificateholder or interactive gaming licensee to conduct interactive gaming in this Commonwealth must be physically located in a secure data center. At least one secondary server must be able to resolve DNS queries.

(b) Redundancy, secondary and emergency servers used by an interactive gaming certificateholder or interactive gaming licensee to conduct interactive gaming in this Commonwealth must be physically located in a secure data center at a separate premises than the primary server.

(c) The Board may require interactive gaming system data necessary to certify revenue and resolve patron complaints to be maintained in the state of Pennsylvania in a manner and location approved by the Board. Such data shall include but not be limited to, 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 shall be maintained in a manner which prevents unauthorized access or modification without the prior approval of the Board.

§ 809.4. Physical and environmental controls for equipment.

(a) Interactive gaming platforms 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 man-made disaster by utilizing and implementing at least the following measures:

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

(2) Secure areas must be protected by appropriate entry controls to ensure that access is restricted to only 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 and attempts at unauthorized access must be logged.

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

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

(d) Interactive gaming system components must provide 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.

§ 809.5. Access to equipment.

(a) The interactive gaming certificateholder and interactive gaming licensee must 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 certificateholder or interactive gaming licensee'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 licensee with prior approval from and as limited by the Board.

(c) All interactive gaming certificateholder's or interactive gaming licensee's interactive gaming systems shall be available for independent testing by the Board, without limitation.

§ **809.6. System requirements.**

(a) An interactive gaming system shall be designed with a methodology (e.g. 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 certificateholder or interactive gaming licensee's interactive gaming system methodology, the Board will consider the following:

(1) The interactive gaming system methodology shall be designed to ensure the integrity and confidentiality of all patron 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 shall 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 shall be encrypted in transit using a method (e.g. AES, IPsec and WPA2) approved by the board.

(3) An interactive gaming certificateholder or interactive gaming licensee shall mask the service set identification of the interactive gaming system network to ensure that it is unavailable to the general public.

(4) All communications that contain patron account numbers, user identification, or passwords and PINs shall utilize a secure method of transfer (e.g. 128-bit key encryption) approved by the Board.

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

(6) Server-based interactive gaming systems shall maintain an internal clock that reflects the current date and time that shall be used to synchronize the time and date between all components that comprise the interactive gaming system. The interactive gaming system date and time shall be visible to the patron when logged on.

(b) Any change or modification to the interactive gaming system, which impacts a regulated feature of an approved gaming system, unless otherwise permitted by the Board, requires submission to and approval by the Board or its designee prior to implementation of the changer or modification.

(c) An interactive gaming system must meet the following standards regarding data logging:

(1) Interactive gaming systems shall 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 such that any logged data is contained in a secure transaction file, a separate logging device is not required.

(2) Interactive gaming systems shall 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 shall electronically log the date and time any Internet or mobile gaming account is created or terminated ("Account Creation Log").

(4) An interactive gaming system shall maintain all information necessary to recreate patron game play and account activity during each patron session, including any identity or location verifications, for a period of no less than 6 years.

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

(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 a gaming

system, the change shall be recorded in a secure electronic log ("Game Availability Log"), which shall 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 shall record all promotional offers ("Promotions Log") issued through the system. Such log shall 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 shall be retained in an electronic log ("Authentication Log") and accessible for a period of not less than 90 days.

(9) All adjustments to gaming system data made using stored procedures shall be recorded in an electronic log ("Adjustments Log"), which lists:

(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 such that there should be no network traffic on a network link which cannot be serviced by hosts on that link.

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

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

(ii) Any intrusion detection system/intrusion prevention system must be installed on the network which can:

(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 if detected.

(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 and/or detection programs 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.

(viv) 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.

(e) The interactive gaming system must implement the self-monitoring or critical components. A critical component that fails self-monitoring tests must 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:

(1) The clocks of all components of the interactive gaming system shall 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 shall be produced and kept for a period of time to be determined by the Board to assist in future investigations and access control monitoring.

(3) System Administrators and System Operator activities shall be logged.

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

(5) Any modifications, attempted modifications, read access or other change or access to any interactive gaming platform 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 shall 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 operator license and an applicant for or holder of an interactive gaming manufacturer license must seek Board approval of all source code used to operate 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) The interactive gaming system must have the following shutdown and recovery capabilities in order to maintain the integrity of the hardware, software and data contained therein in the event of a shutdown:

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

(i) Program resumption routine(s), including self-tests, complete successfully.

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

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

(2) The interactive gaming system must be able to identify and properly handle the situation where 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) An interactive gaming certificateholder or interactive gaming licensee 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 (i.e. "Disaster/Emergency Recovery Plan"). When reviewing the sufficiency of an interactive gaming certificate holder or interactive gaming licensee's plan to recover interactive gaming system operations in the event the interactive gaming system is rendered inoperable, the Board will consider the following:

(i) The Disaster/Emergency Recovery Plan must address the method of storing player account information and gaming data to

minimize loss in the event the interactive gaming system is rendered inoperable. If asynchronous replication is used, the method for recovering data should be described or the potential loss of data should be documented. The Disaster/Emergency Recovery Plan must also:

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

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

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

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

(k) The interactive gaming system must provide an easy and obvious mechanism for players to self-exclude from game play.

(l) The interactive gaming system must provide a mechanism by which a player may be excluded from game play according to the terms and conditions agreed to by the player upon registration.

§ **809.7. Geolocation requirements.**

(a) An interactive gaming system shall employ a mechanism to detect the physical location of a patron upon logging into the interactive gaming system and as frequently as specified in the Board's technical standards and the interactive gaming certificateholder's approved internal controls submission. If the system detects that the physical location of the patron 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 patron until such time that the patron 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 certificateholder or interactive gaming licensee shall 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 the Commonwealth of Pennsylvania unless the conduct of such gaming is not inconsistent with Federal law, law of the jurisdiction, including any foreign nation, in which the participating patron is located, or such gaming activity is conducted pursuant to a reciprocal agreement to which the Commonwealth is a party that is not inconsistent with Federal law.

§ 809.8. Security policy requirements.

Interactive gaming certificateholders and interactive gaming licensees must 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:

(a) Have a provision requiring review when changes occur to the interactive gaming system or the processes which alter the risk profile of the interactive gaming system.

(b) Be approved by the certificateholder's or licensee's management.

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

(d) Undergo review at planned intervals.

(e) 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.