TITLE 68 INDIANA GAMING COMMISSION

Emergency Rule
LSA Document #15-196(E)

DIGEST

Temporarily adds rules regarding limited mobile gaming systems and devices. Statutory authority: IC 4-33-4; IC 4-35-4. *NOTE: The original emergency document, LSA Document #15-82(E), posted at 20150408-IR-068150082ERA, effective April 1, 2015, expires June 30, 2015.* Effective July 1, 2015.

SECTION 1. **(a) This document applies to casino licensees and casino license applicants.**

(b) A mobile gaming device (MGD) is an electronic gaming device and subject to 68 IAC 2-6.

(c) Limited mobile gaming is server-based gaming and subject to 68 IAC 2-6.5.

SECTION 2. **The purpose of this limited mobile gaming system (LMGS) document is to ensure the following:**

(1) Limit the area of LMGS play to authorized gaming areas within the casino.
(2) Limit the MGD's communication to dedicated casino servers.
(3) Protect access to the LMGS to only approved MGDs.
(4) Maintain the public's confidence in regulation and the assurance of heightened integrity and in accordance with IC 4-33, IC 4-35, and 68 IAC.

SECTION 3. **The definitions contained within 68 IAC 1 apply to this document. Additionally, the following definitions apply throughout this document:**

(1) "Authorized gaming area" means the area approved and authorized by the commission to conduct limited mobile gaming.
(2) "Authorized independent gaming laboratory" has the meaning set forth in 68 IAC 2-6-1.
(3) "Cashless wagering system" or "CWS" means a host system whereby a player maintains an electronic account on the casino's host database which allows the play of MGDs through the use of a login and personal identification number (PIN).
(4) "Client terminal" means a device that is used to interact with a gaming system for the purpose of conducting server-based gaming activity. In the context of LMGS, the MGD functions as the client terminal.
(5) "Critical components" means hardware and software required to conduct limited mobile gaming.
(6) "Data library" has the meaning set forth in 68 IAC 2-6.5-1.
(7) "Dormant account" means a limited mobile gaming player account which has had no patron activity for a period of one (1) year.
(8) "Gaming server" means the server that contains game software and control programs. In the context of LMGS, the limited mobile gaming server functions as the gaming server.
(9) "Geo-fence" means a virtual space controlled through a short-range communications protocol such as Wi-Fi. This space corresponds to a physical area in the gaming area within the casino.
(10) "Limited mobile gaming" means the placing of wagers through a wireless server-based gaming system using a computer network through which the casino licensee may offer authorized games to patrons who have established a limited mobile gaming player account with the casino licensee and who are physically present within the defined property boundaries as approved by the commission pursuant to IC 4-33-9-17 and IC 4-35-7-1.5.
(11) "Limited mobile gaming system" or "LMGS" has the meaning set forth in IC 4-33-2-13.3 and IC 4-35-2-7.5.
(12) "Media access control address" or "MAC address" means a unique identifier assigned to network interfaces for communications on the physical network segment. For Wi-Fi, MAC addresses are used as a network address.
(13) "Limited mobile gaming player account" means an account established by a casino licensee that a patron may use for the deposit and withdrawal of funds used for limited mobile gaming.
(14) "Mobile gaming device" or "MGD" has the meaning set forth in IC 4-33-2-13.5 and IC 4-35-2-7.7.
(15) "Peer-to-peer gaming" means gaming in which patrons compete against one other.
(16) "Server-based gaming" means gaming activity conducted via a client terminal where the outcome of a game is determined by a random number generator maintained on a server.
(17) "Server-based gaming system" or "SBGS" means hardware, software, and communications that

comprise a system utilized for the purpose of offering electronic versions of authorized casino games where material aspects of game functionality occur at the server level.

(18) "System administrator" means the IT department personnel responsible for the administration of the LMGS.

(19) "Technology provider" means the vendor, supplier, or manufacturer of one or more components of an LMGS.

(20) "Verification" means a method used by a gaming system or device to verify the validity of software.

(21) "Wi-Fi" means wireless fidelity, which serves as the communication backbone for a wireless network.

SECTION 4. **The executive director or the executive director's designee may approve deviations from the provisions of title 68 IAC upon written request by the person directly affected by the procedure or requirement if the executive director or the executive director's designee determines that the:**

(1) procedure or requirement is impractical or burdensome; and

(2) alternative means of satisfying the procedure or requirement:

(A) fulfill the purpose of the document;

(B) are in the best interests of the public and gaming in Indiana; and

(C) do not violate IC 4-33 or IC 4-35.

SECTION 5. **If the commission determines that a casino licensee or casino license applicant has violated this document, the commission may initiate an investigation and disciplinary action under 68 IAC 13.**

SECTION 6. **The internal control procedures in this document are subject to the following:**

(1) Submission and approval procedures contained within 68 IAC 11-1-3.

(2) Amendment procedures contained within 68 IAC 11-1-4.

(3) Emergency procedures contained within 68 IAC 11-1-5.

SECTION 7. **(a) Casino licensees are required to maintain industry technical standards regarding limited mobile gaming.**

(b) Casino licensees shall meet or exceed the technical standards provided in Gaming Laboratories International Standard 26 – Wireless System Standards (GLI 26), which is hereby incorporated by reference. The incorporated document (Version 2.0, released February 24, 2015) is available for public view at www.gaminglabs.com/en/gli-standards, and copies may be obtained by request mailed to the offices of the Indiana Gaming Commission at 101 West Washington Street, East Tower-Suite 1600, Indianapolis, IN 46204 and does not include any later amendments or editions.

(c) In the event of a conflict between GLI 26 and this document, this document shall prevail.

SECTION 8. **Limited mobile gaming may only be played in the authorized gaming area approved by the commission.**

SECTION 9. **(a) The casino licensee must include the LMGS components within the inventory required by 68 IAC 2-6-6, including the following:**

(1) Hardware and software under the control and responsibility of the technology provider, the casino licensee, and the commission.

(2) Access to hardware or software granted to the casino licensee or technology provider through contracts with third party providers.

(b) The LMGS inventory shall be divided into controlled components, as described in SECTION 13 of this document, and noncontrolled components and shall include the following information:

(1) Identification information for each component, including the following at a minimum:

(A) The serial number assigned to the MGD by the manufacturer.

(B) The registration number issued by the commission.

(C) The name of the manufacturer of the component.

(D) The physical location of the component.

(E) Whether vendor support will be needed to maintain the component.

(2) Documentation of the current topology of the LMGS in the form of network diagrams which illustrate the physical and logical connections between the components of the system.

(3) Wireless network configuration parameters, including, but not limited to, the following:
(A) Addresses.
(B) Host name.
(C) Service set identification.
(D) Encryption.
(E) Related parameter setting.

SECTION 10. **The casino licensee must include approved data files within the electronic repository pursuant to 68 IAC 2-6.5-3.**

SECTION 11. **(a) The system of internal controls of the casino licensee shall, at a minimum, describe the following components of the LMGS:**
(1) LMGS components which record, store, process, share, transmit, or retrieve sensitive player information, including, but not limited to, authentication information and limited mobile gaming player account balances.
(2) LMGS components which generate, transmit, or process random numbers used to determine the outcome of games or virtual events.
(3) LMGS components which store the results or the current state of a player's wager.
(4) Points of entry to and exit from the above systems.
(5) Communication networks which transmit sensitive player information.

(b) Networks serving the LMGS and its components shall be segregated into security domains based on a risk assessment of the functions performed on each network. The risk assessment shall include, but is not limited to, the following:
(1) The devices and software deployed on each network, including, but not limited to, wireless devices, database servers, voice over IP devices, and remote desktop capability.
(2) The value and classification of the information stored or processed in the network.
(3) The access control policy and access requirements for the applications on the network.
(4) Any other requirements imposed by the executive director or the executive director's designee.

(c) The boundaries between networks having different security domains shall be secured from outside traffic. Systems shall be configured to detect and report security-related events at security domain boundaries.

(d) The architecture shall support the use of layered access controls to applications running on the network.

SECTION 12. **MGDs are subject to 68 IAC 2-6, except the following:**
(1) The location of MGDs listed on the electronic gaming device inventory required pursuant to 68 IAC 2-6-6 must designate the location of MGDs as either within the authorized gaming area or within the secured storage area for inactive MGDs.
(2) The notification of electronic gaming device movement pursuant to 68 IAC 17-1-2(d)(1) is only required for MGDs when moved into or out of the authorized gaming area or secured storage area.
(3) The surge protectors required pursuant to 68 IAC 2-6-13(a) shall be required only if MGD charging is permitted by the patron.
(4) The electronic and electromechanical meters and key switch required pursuant to 68 IAC 2-6-9(a) and 68 IAC 2-6-9(d) may be housed on the LMGS server.

SECTION 13. **(a) The casino licensee shall use the LMGS inventory to identify hardware and software components that are used in the operation of the LMGS and shall generate a separate register of controlled components. The authorized independent gaming laboratory which certifies the LMGS will identify the critical files in the software which must form part of the register of controlled components.**

(b) Items in the register of controlled components shall have:
(1) a unique code;
(2) a version number; and
(3) an identification characteristic;
sufficient to ensure that the internal audit department will be able to inspect some or all components at a given time and determine whether they have deviated from the approved version.

(c) A member of the IT department will be assigned responsibility to oversee and perform the

installation of items in the register of configurable assets.

(d) Only the components identified in the LMGS inventory, including the MGDs, and approved by the executive director or the executive director's designee may be used within the LMGS.

(e) Personal devices may not be used to access the LMGS.

SECTION 14. **(a) The LMGS is subject to the requirements of 68 IAC 2-6.5-4 for changes that affect game play or control programs on a LMGD.**

(b) Logging of system changes performed by the casino licensee shall be enabled on databases, and shall record at a minimum the following:
(1) The identity of the user making changes.
(2) The date and time of the modification.
(3) The state of the data prior to the change.
(4) The state of the data after the change.

SECTION 15. **(a) Exception reports shall track events including, but not limited to, the following:**
(1) Adjustments to an authorized player's limited mobile gaming player account balance.
(2) Changes made to information recorded in an authorized player's limited mobile gaming player account.
(3) Voids, overrides, and corrections.
(4) Irrecoverable loss of patron-related data.
(5) Significant periods of system unavailability.
(6) Mandatory deactivation of an authorized player.
(7) Any other activity requiring employee intervention and occurring outside of the normal scope of system operation.

(b) Exception reports produced for the LMGS for the events listed above shall include at a minimum the following:
(1) Date and time of the exception event.
(2) Unique transaction identifier.
(3) Identification of user who performed or authorized alteration.
(4) Data or parameter altered.
(5) Data or parameter value prior to alteration.
(6) Data or parameter value after alteration.
(7) The reason the alteration was made.

SECTION 16. **The casino licensee must submit internal control procedures for the following:**
(1) Maintaining the LMGS inventory.
(2) Ensuring the verification process required by 68 IAC 2-6.5-6 for the LMGS components in the production environment are identical to those approved by the executive director or executive director's designee.
(3) Securing LMGS components.
(4) Accurately accounting for MGDs in addition to the applicable EGD internal control procedures contained within 68 IAC 2-6.

SECTION 17. **(a) The location hosting the gaming server used in association with the LMGS, or that provide redundant facilities for these functions, must be approved by the executive director or executive director's designee and located in the server room within the confines of an approved location described in IC 4-33 or IC 4-35.**

(b) Critical components of the LMGS are to be maintained in secure areas protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

(c) Secure areas where LMGSs are developed, accessed, or maintained shall have physical protection and work guidelines designed and applied.

(d) An uninterruptible power supply to support orderly close down or continuous running shall be supplied for equipment supporting critical business operations.

(e) The physical and environmental security of the LMGS must meet the requirements as outlined in GLI 26.

SECTION 18. **(a) Casino licensees shall utilize an intrusion detection system (IDS) in conjunction with an LMGS. The IDS shall be capable of generating an audit trail report reflecting unauthorized attempts to access the wireless network or a connected MGD. At a minimum, the IT department shall review the audit trail report on a weekly basis. Irregular detections must be noted on the report and shall be reported to the executive director or executive director's designee. The audit trail report is signed and dated by the person reviewing the report.**

(b) Antivirus software shall be deployed on the LMGS to mitigate attacks from known viruses. Logs shall be stored of all virus encounters.

(c) The IDS shall be deployed on the LMGS, and the resulting logs shall be securely stored.

(d) Critical components of the LMGS are to be operational in order for the system to operate. The LMGS shall detect and record information regarding the failure or nonoperation of a component within the system. A log of this event shall be generated.

(e) Audit logs from critical system components and software shall be maintained and shall include the following:

(1) Authorized access, including the following:
- **(A) The user identification.**
- **(B) The date and time of key events.**
- **(C) The types of events.**
- **(D) The files accessed.**
- **(E) The programs or utilities used.**

(2) System alerts or failures, including the following:
- **(A) Console alerts or messages.**
- **(B) System log exceptions.**
- **(C) Changes to the date or time on the network time server.**
- **(D) Network management alarms.**
- **(E) Alarms raised by the access control system.**

(3) Changes to, or attempts to change, system security settings and controls.

SECTION 19. **(a) On a weekly basis, daily system event logs shall be reviewed by internal audit personnel. System event logs shall be maintained for a minimum of seven (7) days following the review.**

(b) The review shall provide reasonable assurance of the following:

(1) Users are only performing activities which have been explicitly authorized.

(2) Possible threats facing the LMGS are being assessed.

(c) Evidence of the review of system event logs is to be maintained for one (1) year. The evidence is to include at a minimum the following:

(1) Date and time of review.

(2) Name and title of person performing the review.

(3) The system event log reviewed.

(4) Any exceptions, follow-up, and resolution of exceptions.

SECTION 20. **(a) Networks serving an LMGS and its components shall be secure from outside traffic and systems shall be configured to detect and report security-related events.**

(b) Network shared drives containing application files and data for the LMGS shall be secured such that only authorized personnel may gain access.

(c) Login accounts and passwords required to administer network and other equipment shall be secured such that only authorized IT personnel may gain access to these devices. The passwords for these accounts shall meet minimum required security parameters, and accounts shall be immediately disabled when IT personnel are terminated.

(d) The casino licensee shall mask the service set identification of the LMGS network to ensure that it

is not available for broadcast to the public.

SECTION 21. **(a) The LMGS is subject to the security and surveillance rules contained within 68 IAC 12. In the event of a conflict between 68 IAC 12 and this document, the provisions outlined in this document shall prevail.**

(b) The surveillance system must provide an overall view of the LMGS gaming area capable of clearly identifying the following:

(1) LMGS casino employees at the LMGS registration.

(2) Facial view of a patron registering for a limited mobile gaming player account with sufficient clarity to allow identification of the patron.

(3) Facial view of a patron checking out or checking in a MGD with sufficient clarity to allow identification of the patron.

(4) The amount deposited into a limited mobile gaming player account.

(5) Points of ingress to and egress from the LMGS gaming area.

(c) The surveillance system must include cameras dedicated to monitoring the registration area where the MGDs are stored prior to being checked out.

(d) The surveillance system must include cameras dedicated to monitoring points of access to the room housing the LMGS servers.

(e) The surveillance system must include cameras dedicated to monitoring points of access to any other location where MGDs are stored.

SECTION 22. **The casino licensee must submit internal controls to maintain all aspects of security, including the following:**

(1) Procedures to handle different types of security incidents, including the following:

(A) System failures and loss of service.

(B) Malicious code detection.

(C) Denial of service.

(D) Errors resulting from incomplete or inaccurate business data.

(E) Breaches of confidentiality or integrity.

(F) Misuse of information systems.

(2) In addition to the normal contingency plans, these internal controls shall include the following:

(A) Analysis and cause of the security incident.

(B) Containment.

(C) Planning and implementation of corrective action to prevent recurrence.

(D) Communication with those affected by or involved with recovery from the security incident.

(E) Reporting of the action to the executive director or executive director's designee.

(3) Action to recover from security breaches and correct system failures shall be carefully and formally controlled; the procedures shall ensure the following:

(A) Only clearly identified and authorized personnel are allowed access to live systems and data.

(B) Emergency actions taken are documented in detail.

(C) Emergency action is reported to management and reviewed in an orderly manner.

(D) The integrity of business systems and controls is confirmed with minimal delay.

(4) Testing the integrity of the LMGS on an ongoing basis.

SECTION 23. **The LMGS, including application software, shall be secured through the use of passwords, biometrics, or other suitable means.**

SECTION 24. **(a) The system administrator shall establish, revise, and deactivate user accounts.**

(1) Application functions for a user shall be limited to the user's current job responsibilities.

(2) User accounts shall be disabled upon employee termination or change in employee job responsibilities that no longer require access to the LMGS within twenty-four (24) hours of termination or change.

(b) Security parameters for passwords shall, at a minimum, meet industry technical standards.

SECTION 25. **(a) The casino licensee shall request approval from the executive director or executive director's designee for instances of remote access at least twenty-four (24) hours before access is**

requested. The request shall include the following:

(1) The LMGS components requiring vendor support and the name of the licensed supplier.

(2) The purpose for remote access.

(b) Remote access shall be restricted to support or updates and include only the applications and databases that are necessary.

(c) In the event an emergency exists, the casino licensee shall contact the commission office on property for authorization.

SECTION 26. **(a) An instance of remote access to the LMGS components shall be automatically logged by the device or software when it is established. At a minimum, the log must include the following:**

(1) Name of user account through which the system was accessed.

(2) Date, time, and duration of the access.

(b) A complete log of remote access must be created by the casino licensee and include at a minimum the following:

(1) Commission staff authorization.

(2) Name or identifier of the system administrator that requested remote access.

(3) Name of licensed supplier.

(4) Name and license number of licensed supplier employee that accessed the LMGS.

(5) System components accessed by the licensed supplier employee.

(6) Detailed description of work performed.

(7) Date, time, and duration of access.

SECTION 27. **(a) System documentation for in-use components of the LMGS shall be maintained.**

(b) The casino licensee shall document the responsibilities of the IT department for the maintenance of the components of the LMGS. The documentation shall include the following:

(1) The roles of IT personnel in performing routine and nonroutine maintenance on the components of the LMGS.

(2) The source of procedures for performing routine maintenance activities.

(3) The records of the maintenance activities required to be kept.

(c) LMGS equipment shall be correctly maintained to ensure its continued availability and integrity.

(d) Documentation records shall be kept for one (1) year.

SECTION 28. **The casino licensee must submit internal controls for the following:**

(1) Access privileges to the LMGS that include, but are not limited to, the following:

(A) Access to a component of the LMGS shall be configured to prevent the transfer of personally identifiable information outside of the casino.

(B) Access shall be continuously monitored by the casino licensee.

(2) Subsequent to an authorized use by a licensed supplier, the account shall be returned to a disabled state on all operating systems, databases, network devices, and applications until needed by such licensed supplier and approved by the executive director or executive director's designee.

(3) Remote access to the LMGS and its components for purposes of licensed supplier support must include the following:

(A) The method and procedures used to gain access remotely, including the use of passwords and other logical controls, and commission staff observation.

(B) The procedures to be used by the IT department to further control and monitor access and to ensure that licensed suppliers have only the limited access needed to perform authorized support and update functions.

SECTION 29. **(a) MGDs shall be stored where they will be secured, remain under surveillance, and individually logged by the registration number assigned by the executive director or executive director's designee.**

(b) IT will associate the MGD's MAC address to the gaming server via the network.

(c) The MAC address will remain inactive until the MGD is linked to a limited mobile gaming player account when the MGD is checked out for a gaming session.

(d) MGDs will be tracked and stored by an individual active sequential inventory control number.

(e) The MGD's MAC address shall become active only when the MGD is distributed to a patron and linked with the patron's limited mobile gaming player account. As active MGDs are distributed, the inventory control number of the device will be electronically noted in the limited mobile gaming player account until the device is returned.

(f) Surplus inventory will be stored and logged by unique MAC address in a separate locked area of the casino.

(g) Stored MGDs will be inactive and restricted from the server.

(h) MGD security shall ensure the following:
(1) MGDs are not operational beyond the confines of the geo-fence.
(2) Surveillance of the authorized gaming area points of ingress and egress is maintained.
(3) A valid limited mobile gaming player account is a prerequisite for checking out a device.
(4) Signage is prominently displayed at the casino to indicate the boundaries of the authorized gaming areas.
(5) MGD splash screens provide for electronic acknowledgement of official rules for LMGS.
(6) MGD becomes inactive after fifteen (15) minutes of inactivity.
(7) Stolen or lost MGDs are marked as disabled.

SECTION 30. **(a) Active MGDs that are not working or that have a malfunction that cannot be immediately addressed by dispatched IT technicians will be marked for repair on the active MGD log.**

(b) Casino IT shall disassociate the MAC address of the MGD in need of repair with the server so the device is inactive during repair.

(c) As MGDs are repaired, the MAC address will be reassociated with the server, the active device log will be updated, and the active device will be placed back into active service.

SECTION 31. **(a) If an MGD needs replaced, casino IT will complete a destruction form.**

(b) Commission gaming agents, surveillance, and security shall be notified by IT to witness destruction of the device.

(c) Casino IT will disassociate the MAC address of the MGD in need of replacement via the network and reassociate a new MGD from the surplus stock.

(d) The active device log shall be updated, the destruction form filed, and the new active MGD will go into service assuming the same inventory control number and docking slot as the replaced device.

SECTION 32. **(a) LMGS equipment containing storage media shall be checked to ensure that sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse in a separate area of the business.**

(b) Storage media shall be disposed of securely and safely when no longer required.

(c) A record of the disposal of equipment or media shall be kept in the LMGS inventory.

SECTION 33. **The casino licensee must submit internal controls to ensure the following:**
(1) Malfunctioning MGDs are removed from active service and repaired without affecting the LMGS.
(2) Repaired MGDs are returned to active service without affecting the LMGS.
(3) MGDs permanently removed from service shall be destroyed or disposed of according to a plan approved by the executive director or executive director's designee.

SECTION 34. **The LMGS shall employ a continuous mechanism to detect the physical location of the MGD. If the system detects that the physical location of the MGD is in an area unauthorized for limited**

mobile gaming, the LMGS shall not accept wagers and shall disable the patron's MGD for play until such time that the patron is in an authorized location as follows:

(1) The play of games on the LMGS will be restricted to an authorized gaming area of the casino as approved by the executive director or executive director's designee. An LMGS shall disable wagering activity on a client terminal whenever it is removed from the confines of the authorized gaming area.

(2) MGDs will only be allowed to connect to the LMGS within this defined authorized gaming area. The wireless network will have Wi-Fi geo-fence technology to ensure the devices do not operate outside of this allowed footprint. The area will be monitored by the surveillance department via video cameras to further ensure adherence to the authorized gaming areas of LMGS-based play.

(3) Only MGDs authorized by the executive director or executive director's designee shall be permitted to establish communications with the LMGS.

SECTION 35. **(a) MGDs shall incorporate a location tracking component to track the location of a MGD to detect when a device has been transported out of the authorized gaming area.**

(b) The location tracking component shall provide the surveillance department with the location of a MGD within a twenty (20) feet by twenty (20) feet area.

(c) When a device is removed from the authorized gaming area, the LMGS shall disable a current gaming or casino licensee sessions associated with that device.

(d) A casino licensee may hold an MGD for a patron subject to the requirements of 68 IAC 10-1-1.2.

SECTION 36. **Prior to establishing a player session, the LMGS must be able to authenticate the authorized player requesting to establish a session using an electronic identifier such as a digital certificate or an account description and password. If the LMGS is unable to reasonably authenticate the authorized player after three (3) consecutive attempts, the LMGS must use strong or multifactor authentication upon the next request to authenticate the authorized player. Upon establishing a new player session, the LMGS must notify the authorized player of the last time the account was logged in.**

SECTION 37. **In addition to 68 IAC 2-6 and 68 IAC 2-6.5, casino licensees shall ensure that the following requirements are met with respect to theme activation:**

(1) MGDs shall not contain logic utilized to generate the result of a game. All critical functions including the generation of a game outcome shall be generated by the LMGS game server.

(2) MGDs must not be capable of conducting a gaming activity if disconnected from the LMGS or if communications with the LMGS is severed.

(3) MGDs must not be used to store sensitive data or system information.

(4) MGDs must not automatically alter client-specific firewall rules to open ports that are otherwise blocked by a hardware or software firewall.

(5) MGDs shall not access ports which are not required for client or server communications.

(6) MGDs must not be able to transfer data to other wireless clients except in peer-to-peer gaming or other executive director or executive director's designee approved functions.

(7) Nongame-related functionality supported by MGDs must not impact the gaming data integrity and be approved by the executive director or executive director's designee.

(8) Game outcome must not be impaired by:

(A) bandwidth;

(B) link utilization;

(C) bit error rate; or

(D) other communication characteristics that exist between MGDs and the LMGS server.

(9) Individual par sheets for a game must be kept on file and accessible to the executive director or executive director's designee before the MGD can be released for play.

SECTION 38. **The LMGS must be able to terminate a game or player session under the following conditions and notify the player of the termination:**

(1) An authorized player voluntarily terminates the session.

(2) An authorized player fails authentication during a game or player session.

(3) A user-inactivity timeout is reached.

(4) The LMGS is unable to verify the connection status of an authorized player after a reasonable number of attempts.

(5) A limit of the limited mobile gaming player account has been reached.

(6) The casino licensee manually terminates the session.

(7) The executive director or executive director's designee requests termination.
(8) Any other reason as determined by the executive director or executive director's designee.

SECTION 39. **Only games authorized by 68 IAC 1-16-4 and 68 IAC 2-6-22 are permitted.**

SECTION 40. **(a) For the base system, the following documentation shall be available upon request by the executive director or executive director's designee:**
(1) A list of individual games hosted or offered on the LMGS.
(2) An all-inclusive functional description of the LMGS.

(b) For games that run on the LMGS, the following documentation must be available:
(1) Game name.
(2) Game version numbers.
(3) Paytable identification numbers.
(4) Detailed game rules, including options and bonus features.
(5) Detailed breakdown of paytables, payouts, and mapped symbols present in the game.
(6) A list of active devices currently installed on the server.

(c) Game rules shall be available for inspection upon request by a patron.

SECTION 41. **For an individual game played, the following information shall be recorded, maintained, and easily demonstrable by the LMGS:**
(1) A unique player identification.
(2) The contributions to progressive jackpot pools.
(3) The game status.
(4) The paytable used.
(5) The game identifier and version.
(6) The date and time the game started and ended.
(7) The display associated with the final outcome of the game, either graphically or via a clear text message.
(8) The total player cash or credits at start and end of play.
(9) The total amount bet.
(10) The total cash or credits won for the prize.
(11) The results of player choices involved in the game outcome.
(12) The results of intermediate game phases.
(13) The amount of promotional awards received.

SECTION 42. **The casino licensee must maintain and back up a log of limited mobile gaming player account activity.**

SECTION 43. **The casino licensee's LMGS terms and conditions must clearly define its policies in respect of unrecoverable malfunctions of gambling hardware or software including components of the LMGS.**

SECTION 44. **The casino licensee shall have the ability to disable any game or game session without unfair impact on the patron. The casino licensee shall provide full audit trails when disabling a game that is currently in play.**

SECTION 45. **The casino licensee shall implement a user inactivity timeout that automatically logs the patron out and/or ends the patron's session after a fifteen (15) minute period of inactivity.**

SECTION 46. **(a) For games that can have multiple stages, the LMGS shall provide a method for the patron to return to an incomplete game to complete it.**

(b) The casino licensee must provide a mechanism for a patron to complete an incomplete game before a patron is permitted to participate in another game. Incomplete games may occur as a result of the following:
(1) Loss of communications between LMGS network and player MGD.
(2) System restart condition.
(3) Game disablement.
(4) MGD restart.

(5) Abnormal termination of gambling application on MGD.

(c) Gambling associated with a partially complete game that can be continued and completed within a reasonable time must be held by the casino licensee until the game completes. Limited mobile gaming player accounts must reflect funds held for incomplete games.

(d) The casino licensee must ensure patron fairness, to the extent possible, in the event of a communication loss to one or more MGDs during a multipatron game, if applicable.

(e) Game rules must provide for situations where the casino licensee loses connectivity with the patron device.

SECTION 47. **The casino licensee must submit internal controls to ensure that service interruptions are fairly handled.**

SECTION 48. **(a) Before allowing or accepting wagers from a patron to engage in limited mobile gaming, a casino licensee must register the individual as an authorized player and create a limited mobile gaming player account for the patron.**

(b) A casino licensee may register a patron as an authorized player only if the patron provides the casino licensee with the following information:
(1) A government issued identification.
(2) The patron's date of birth showing that the individual is twenty-one (21) years of age or older.
(3) The physical address where the patron resides.

(c) Before registering a patron as an authorized player, the casino licensee must have the patron affirm the following:
(1) That the information provided to the casino licensee by the patron to register is accurate.
(2) That the patron has reviewed and acknowledged access to the house rules and terms and conditions for limited mobile gaming.
(3) That the patron has been informed and has acknowledged that, as an authorized player, he is prohibited from allowing another person access to or use of his limited mobile gaming player account or MGD.

(d) Before registering a patron as an authorized player, the casino licensee must confirm that the patron is not:
(1) an excluded person pursuant to 68 IAC 6-1; or
(2) a voluntarily excluded person pursuant to 68 IAC 6-3.

SECTION 49. **(a) A casino licensee shall record and maintain the following in relation to a limited mobile gaming player account:**
(1) The date and time the limited mobile gaming player account is opened and terminated.
(2) The date and time the limited mobile gaming player account is logged into or is logged out of.

(b) The casino licensee shall ensure that a patron registered as an authorized player holds only one (1) limited mobile gaming player account with the casino licensee.

(c) A casino licensee shall not set up anonymous limited mobile gaming player accounts or accounts in fictitious names.

(d) Funds may be deposited by an authorized player into a limited mobile gaming player account as follows:
(1) Cash, as defined in 68 IAC 1-1-12, deposited directly with the casino licensee.
(2) Cash equivalents, as defined in 68 IAC 1-1-13, deposited directly with the casino licensee.

(e) Limited mobile gaming player account credits may be made by the following means:
(1) Deposits.
(2) Amounts won by an authorized player.
(3) Promotional credits, or bonus credits provided by the casino licensee and subject to the terms of use established by the casino licensee and as long as such credits are clearly identified as such.
(4) Adjustments made by the casino licensee following the resolution of a dispute.

(f) Limited mobile gaming player account debits may be made by the following means:
(1) Amounts wagered by an authorized player.
(2) Purchases of limited mobile gaming related merchandise and services requested by an authorized player.
(3) Withdrawals.
(4) Transfers to safekeeping or front money accounts held by the casino licensee.
(5) Adjustments made by the casino licensee following the resolution of a dispute.
(6) Debits as otherwise approved by the executive director or executive director's designee.

(g) Unless there is a pending unresolved player dispute or investigation, a casino licensee shall comply with a request for a withdrawal of funds by an authorized player from the limited mobile gaming player account within a reasonable amount of time.

(h) A casino licensee shall not allow an authorized player to transfer funds to another authorized player.

(i) The language of an agreement, including, but not limited to, house rules or terms and conditions, used between a casino licensee and its authorized players pertaining to limited mobile gaming and authorized players' access to the limited mobile gaming player account shall be submitted to the executive director or executive director's designee for approval. The casino licensee shall not allow or engage in limited mobile gaming until such agreement is approved by the executive director or executive director's designee.

(j) A casino licensee shall ensure that an authorized player has the ability, through the limited mobile gaming player account, to select responsible gambling options that include the following without limitation:
(1) Loss limits establishing the net loss that can occur within a specified period of time.
(2) Deposit limits establishing the amount of total deposits an authorized player can make to the limited mobile gaming player account within a specified period of time.
(3) Tournament limits establishing the total dollar amount of tournament entries an authorized player can purchase within a specified period of time.
(4) Play time limits establishing the total amount of time available for play during a specified period of time.

(k) Nothing in this document prohibits a casino licensee from closing a limited mobile gaming player account and precluding further limited mobile gaming by an authorized player pursuant to the terms of the agreements between the casino licensee and an authorized player.

SECTION 50. **Adjustments to limited mobile gaming player accounts shall be authorized by supervisory personnel.**

SECTION 51. **(a) Transactions must be identifiable and maintained in a system audit log.**

(b) A deposit into a limited mobile gaming player account must not be available for gambling until such time as the transaction has been approved by the appropriate issuing authority. This authorization must be maintained in a system audit log.

(c) Casino licensees must provide information to patrons about whether the casino licensee protects patron funds and the methods it uses to do so and about how it deals with unclaimed funds from dormant accounts.

SECTION 52. **The casino licensee shall provide an account statement with account details to a patron on demand. The account statement shall include detailed account activity for a defined time period. Information to be provided shall include, at a minimum, the following:**
(1) Deposits to the limited mobile gaming player account.
(2) Withdrawals from the limited mobile gaming player account.
(3) Lifetime win or loss totals.
(4) Current account balance.
(5) Self-imposed limit history, if applicable.

SECTION 53. **A casino licensee shall notify the limited mobile gaming player account holder via electronic mail, regular mail, or other method approved by the executive director or executive director's designee, whenever the limited mobile gaming player account has been deactivated or placed in a suspended mode. Such notification shall include the restrictions placed on the account and further course of action needed to remove the restriction.**

SECTION 54. **The casino licensee must submit internal controls for the following:**

(1) Registering authorized players to engage in limited mobile gaming.

(2) Identifying and verifying authorized players to prevent those who are not authorized players from engaging in limited mobile gaming.

(3) Ensuring compliance related to child support obligors pursuant to IC 4-33-4-27 and IC 4-35-4-16.

(4) Protecting and ensuring confidentiality of authorized players' limited mobile gaming player accounts.

(5) Issuing, modifying, and resetting a patron's limited mobile gaming player account password, personal identification number, or other approved security feature, where applicable.

(6) Promoting responsible limited mobile gaming.

SECTION 55. **(a) An LMGS shall utilize sufficient security to ensure patron access is appropriately limited to the account holder. Security measures shall include the following:**

(1) Personal identification number.

(2) Password or other access security feature.

(3) Two (2) or more challenge questions.

(4) Password expiration every quarter.

(b) The LMGS shall utilize a secure method of data transfer approved by the executive director or executive director's designee for communications that contain the following:

(1) Patron account numbers.

(2) User identification.

(3) Passwords.

(4) Personal identification numbers.

SECTION 56. **For an internal or external CWS, the following applies:**

(1) The CWS must communicate acceptance, partial acceptance, or rejection of wagers placed through play of games on the LMGS.

(2) When the CWS determines the cost of the wager, there is a positive confirmation sequence in place to ensure the following:

(A) Enable the patron to accept the wager cost.

(B) Confirm there are enough funds in the patron's limited mobile gaming player account to meet the wager cost.

(3) If the patron accepts the wager, the CWS shall complete the following actions:

(A) Debit the patron's limited mobile gaming player account in the amount equal to the cost of the wager.

(B) Retain the funds as a pending transaction.

(C) Log details of the cost of the wager.

(4) If the patron cancels the wager, the CWS shall complete the following actions:

(A) Communicate acknowledgement of acceptance or rejection of the cancellation request to the patron.

(B) Log details of the cancellation request.

(5) When the result is entered and confirmed, the CWS shall transfer the winning wager placed from the LMGS back to the LMGS with the amount of the win.

(6) Upon receiving the CWS win confirmation, the LMGS shall update the patron's limited mobile gaming player account with the winning amount, less required withholding amount.

SECTION 57. **The casino licensee must submit internal control procedures to ensure that LMGS accounting records and procedures meet the requirement in 68 IAC 15-1, including, but not limited to, the following:**

(1) Tax required to be paid by the casino licensee pursuant to IC 4-33 and IC 4-35.

(2) Jackpots.

SECTION 58. **(a) Wagering by an individual that is not the registered player account holder assigned to the particular MGD, regardless of permission by the player account holder, is void.**

(b) Winnings related to wagers by a nonregistered player account holder are forfeited.

(c) The forfeited winnings will be withheld by the casino licensee and remitted to the commission. The commission shall collect the winnings. The registered player account holder may appeal a forfeiture under this SECTION by following the procedures outlined in 68 IAC 7.

SECTION 59. **The casino licensee shall implement appropriate internal controls to identify and prohibit the following existing limited mobile gaming player accounts from placing a wager:**

(1) Voluntarily excluded patrons.
(2) Patrons on the exclusion list.
(3) Patrons with deactivated accounts.
(4) Patrons with suspended accounts.

SECTION 60. This document shall take effect July 1, 2015.

LSA Document #15-196(E)
Filed with Publisher: June 29, 2015, 2:32 p.m.
Documents Incorporated by Reference: Gaming Laboratories International, Standard Series, GLI 26: Wireless Systems Standard, Version 2.0, February 24, 2015

Posted: 07/01/2015 by Legislative Services Agency
An html version of this document.