LOUISIANA

ADMINSTRATIVE CODE

TITLE 42

LOUISIANA GAMING

NOVEMBER 2018

UPDATE

Internal Controls; Table Games
This amended LAC 42:III.2717

Internal Controls; Slots
This amended LAC 42:III.2723

Casino Computer Systems
This adopted LAC 42:III.Chapter 28 (§§ 2801 – 2825)

Computer Monitoring Requirements of Electronic Gaming Devices
This repealed LAC 42:III.4205

without the unacceptable or invalid provisions, and to that end the provisions of this order are severable.

B. This order (Statewide Order No. 29-R-18/19) supersedes Statewide Order No. 29-R-17/18 and any amendments thereof.

AUTHORITY NOTE: Promulgated in accordance with R.S. 30:21 et seq.

HISTORICAL NOTE: Promulgated by the Department of Natural Resources, Office of Conservation, LR 14:544 (August 1988), amended LR 15:552 (July 1989), LR 21:1251 (November 1995), LR 24:459 (March 1998), LR 24:2128 (November 1998), LR 25:1874 (October 1999), LR 26:2305 (October 2000), LR 27:1921 (November 2001), LR 28:2368 (November 2002), LR 29:2502 (November 2003), LR 30:2494 (November 2004), LR 31:2950 (November 2005), LR 32:2088 (November 2006), LR 33:2462 (November 2007), LR 34:2406 (November 2008), LR 35:2464 (November 2009), LR 36:2570 (November 2010), LR 37:3274 (November 2011), LR 38:2931 (November 2012), LR 39:3100 (November 2013), LR 40:2267 (November 2014), LR 41:2379 (November 2015), LR 42:1959 (November 2016), LR 43:2191 (November 2017), LR 44:2013 (November 2018).

Richard P. Ieyoub
Commissioner

1811#012

RULE

Department of Public Safety and Corrections
Gaming Control Board

Casino Computer Systems
(LAC 42:III.2717, 2723, and Chapter 28)

The Department of Public Safety and Corrections, Louisiana Gaming Control Board, in accordance with R.S. 27:15, R.S. 27:24, and the provisions of the Administrative Procedure Act, R.S. 49:950 et seq., hereby gives notice that it has adopted LAC 42:III.Chapter 28, Casino Computer Systems. This will include a regulation reorganization by consolidating Subsection N of §2717, Subsection Q of §2723, and §4205, all located in LAC 42:III, within the new Chapter 28 of LAC 42:III, as the changes create uniformity so that all data breach and information systems can be in a consolidated Chapter.

The Gaming Control Board has amended LAC 42:III.2717 by repealing Subsection N and replacing Subsection O as the new Subsection N. The amendment will maintain the division's access to all of information pertaining to table games that is maintained by the licensees. Further, the Gaming Control Board has amended LAC 42:III.2723 by repealing Subsection Q and replacing Subsection R as the new subsection Q and by replacing Subsection S as the new Subsection R. Additionally, the Gaming Control Board has repealed LAC 42:III.4205 as part of the regulation reorganization into LAC 42:III.Chapter 28.

The Sections in Chapter 28 have been promulgated in order to protect patron data from data breaches. With the advancements in technology, riverboat licensees and the casino operator are using computer systems to keep track of all player data and rewards, and credit information when issuing markers. Due to this, they are collecting massive amounts of confidential data on patrons. The rules do not currently address how the licensees should protect this data and what system protections they should have. Considering recent data breaches among companies nationwide, the board and division deemed it necessary to implement rules to safeguard the confidential information. This Rule is hereby adopted on the day of promulgation.

Title 42
LOUISIANA GAMING
Part III. Gaming Control Board
Chapter 27. Accounting Regulations

§2717. Internal Controls; Table Games

A - M.1. ...

N. Table Games Records

1. Each licensee and casino operator shall maintain records and reports reflecting drop, win and drop hold percentage by table and type of game by day, cumulative month-to-date, and cumulative year-to-date. The reports shall be presented to and reviewed by management independent of the pit department on at least a monthly basis. The independent management shall investigate any unusual statistical fluctuations with pit supervisory personnel. At a minimum, investigations are performed for all statistical percentage fluctuations from the base level for a month in excess of plus or minus three percentage points. The base level is defined as the licensee's or casino operator's statistical win to statistical drop percentage for the previous business year. The results of such investigations shall be documented in writing and maintained for at least five years by the licensee.

2. The division shall have access to all information pertaining to table games.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 38:1635 (July 2012), amended LR 44:2014 (November 2018).

§2723. Internal Controls; Slots

A. - P.1. ...

Q. The accounting department shall perform the following audit procedures relative to slot operations:

1. collect jackpot and hopper fill slips, computerized and manual, and other paperwork daily from the locked accounting box and the cashier cage or as otherwise approved by the division;

2. review jackpot and fill slips daily for continuous sequence. Ensure that proper procedures were used to void slips. Investigate all missing slips and errors. Document the investigation and retain the results for a minimum of five years;

3. manually add, on a daily basis, all jackpot and fill slips and trace the totals from the slips to the system-generated totals. Document all variances and retain the documentation for five years;

4. collect the hard count and currency acceptor count results from the count teams and compare the actual count to the system-generated meter reports on a daily basis;

5. prepare reports of their daily comparisons by device, by denomination, and in total of the actual count for hard and soft count to system-generated totals. Report variance(s) of $100 or greater to the slot department for investigation. Maintain a copy of these reports for five years;

6. compare a listing of slot machine numbers scheduled to be dropped to a listing of slot machine numbers actually counted to ensure that all drop buckets and currency acceptors are accounted for during each drop period;

7. immediately investigate any variance of 2 percent or more per denomination between the weigh or count and wrap. Document and maintain the results of such investigation for five years;

8. compare 10 percent of jackpot and hopper fill slips to signature cards for proper signatures one day each month;

9. compare the weigh tape to the system-generated weigh, as recorded in the slot statistical report at least one drop period per month. Resolve any discrepancies prior to generation and distribution of slot reports to management;

10. review the weigh scale tape of one gaming day each quarter to ensure that:

a. all electronic gaming device numbers were properly included;

b. only valid identification numbers were accepted;

c. all errors were investigated and properly documented, if applicable;

d. the weigh scale correctly calculated the dollar value of coins; and

e. all discrepancies are documented and the documentation is maintained for a minimum of five years;

11. verify the continuing accuracy of the coin-in meter readings as recorded in the slot statistical report at least monthly;

12. compare the "bill-in" meter reading to the currency acceptor drop amount at least monthly. Discrepancies shall be resolved prior to the generation and distribution of slot statistical reports to management;

13. maintain a personnel access listing for all computerized slot systems which includes, at a minimum:

a. employee name;

b. employee identification number, or equivalent; and

c. listing of functions the employee can perform or equivalent means of identifying same;

14. review sensitive key logs. Investigate and document any omissions and any instances in which these keys are not signed out and signed in by the same individual;

15. on a daily basis, review exceptions, jackpot overrides, and verification reports for all computerized slot systems, including tokens, coins and currency acceptors, for propriety of transactions and unusual occurrences. These exception reports shall include the following:

a. cash variance which compares actual cash to metered cash by machine, by denomination and in total;

b. drop comparison which compares the drop meter to weigh scale by machine, by denomination and in total.

R. Slot Department Requirements

1. The slot booths, change banks, and change banks incorporated in beverage bars (bar banks) shall be counted down and reconciled each shift utilizing appropriate accountability documentation.

2. The wrapping of loose slot booth and cashier cage coin shall be performed at a time or location that does not interfere with the hard count process or the accountability of that process.

3. A record shall be maintained evidencing the transfers of unwrapped coin.

4. Slot booth, change bank, and bar bank token and chip storage cabinets and drawers shall be constructed to provide maximum security of the chips and tokens.

5. Each station shall have a separate lock and shall be keyed differently.

6. Slot booth, change bank, and bar bank cabinet and drawer keys shall be maintained by the supervisor and issued to the change employee assigned to sell chips and tokens. Issuance of these keys shall be evidenced by a key log, which shall be signed by the change employee to whom the key is issued. All slot booth, change bank, and bar bank keys shall be returned to the supervisor at the end of each shift. The return of these keys shall be evidenced on the key log, which shall be signed by the cage employee to whom the key was previously issued. The key log shall include:

a. the change employee's employee number and signature;

b. the date and time the key is signed out; and

c. the date and time the key is returned.

7. At the end of each shift, the outgoing and incoming change employee shall count the bank. The outgoing employee shall fill out a count sheet, which shall include opening and closing inventories listing all currency, coin, tokens, chips and other supporting documentation. The count sheet shall be signed by both employees.

8. In the event there is no incoming change employee, the supervisor shall count and verify the closing inventory of the slot booth, change bank, and bar bank.

9. Increases and decreases to the slot booths, change banks, and bar banks shall be supported by written documentation signed by the cage cashier and the slot booth, change bank, or bar bank employee.

10. The slot department or MIS shall maintain documentation of system-related problems, including, but not limited to, system failures, extreme values for no apparent reason, and problems with data collection units, and document the follow-up procedures performed. Documentation shall include at a minimum:

a. date the problem was identified;

b. description of the problem;

c. name and position of person who identified the problem;

d. name and position of person(s) performing the follow up;

e. date the problem was corrected; and

f. how the problem was corrected.

11. The slot department shall investigate all meter variances received from accounting. Copies of the results of the slot department's investigation shall be retained by the accounting department for five years.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 38:1641 (July 2012), amended LR 44:2014 (November 2018).

Chapter 28. Casino Computer Systems

§2801. Protection and Security of Information and Information Systems

A. This Chapter applies to all systems of an operation that includes a casino and common ownership, except that any non-gaming systems that are segregated from any and all gaming systems and from which one cannot access any gaming systems shall be exempt from the provisions of this section. The requirements in this Chapter are in addition to

existing state and federal regulations. Unrelated third party operating systems independent from the licensee, casino operator, and other related businesses are responsible for protecting patron information in accordance with state and federal laws and regulations.

B. Each licensee and casino operator shall:

1. implement an information security program that addresses the managerial, operational, and technical aspects of protecting information and information systems; and

2. develop, document, audit, and enforce an information security plan consisting of policies, guidelines, standards, processes, and procedures in accordance with the law and regulation. The policy shall include a risk assessment designed to, among other things, identify threats and vulnerabilities and methods to mitigate the associated risks. Additionally, the policy shall include controls over both timing (preventive, detective, and corrective) and nature (administrative, technical, and physical).

C. Computer systems shall be designed and implemented to safeguard the security, confidentiality, integrity, and availability of information systems and the information processed, stored, and transmitted by those systems to prevent security incidents. A security incident is any attempted or successful occurrence that jeopardizes the security, confidentiality, integrity, or availability of information systems and the information processed, stored, or transmitted by those systems. A security incident includes, but is not limited to: the unauthorized release of data (including personal patron data) collected, stored, and/or maintained by a licensee and casino operator; unavailability or degradation of services; misappropriation or theft of information or services; and modification or destruction of systems or information.

D.1.A licensee and casino operator shall:

a. identify and correct information and information system defects in a timely manner;

b. provide protection from malicious code at appropriate locations within the casino's information systems; and

c. monitor information system security alerts and advisories and take appropriate actions in response thereto.

2. The network system shall have the capacity to detect and display the following conditions:

a. power reset or failure of any network component;

b. communication loss between any network components; and

c. authentication failure.

3. Any defects or anomalous conditions shall be recorded in an error log that shall be displayed or printed upon demand by the board or division and shall be maintained for a period of three years.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2015 (November 2018).

§2803. Assessment Audits

A. A licensee and casino operator shall develop and maintain computer systems and procedures in compliance with standards recognized as industry accepted "information security standard" as selected by the licensee or casino operator.

B. A licensee and casino operator shall, no later than 36 months from its last assessment, submit the results of an independent network security risk assessment to the division for review, subject to the following requirements:

1. the testing organization must be independent of the licensee and casino operator;

2. results from the network security risk assessment shall be submitted to the division no later than 90 days after the assessment is conducted.

C. At the discretion of the division, additional network security risk assessments may be required.

D. A licensee and casino operator shall periodically, but no later than 36 months from its last assessment, assess the risk to operations, assets, patrons, employees, and other individuals or entities resulting from the operation of the casino's computer systems and the processing, storage, or transmission of information and data. The assessment shall be documented and recorded in a manner that can be displayed or printed upon demand by the board or division and shall be maintained for a period of five years. Licensees and casino operators shall assess the collection of personnel and patron data annually to ensure that only information necessary for the operation of the business is collected and maintained. No unnecessary personal information shall be retained.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2016 (November 2018).

§2805. Notification and Response Time

A. A licensee and casino operator shall provide written notice of the following to the division within 24 hours:

1. discovery that a system or data has been compromised;

2. suspicion or notification from outside sources that a system or data may have been compromised; or

3. determination that a system or data has been otherwise accessed or released without proper authorization.

B. Confirmed breaches of any systems related to the Louisiana properties or any other company owned by common ownership shall be disclosed to the board with 24 hours of confirmation. The notification shall provide all known details at the time of notification including, but not limited to, the location(s) affected and the process that will be used to move forward with the investigation.

C. Upon confirming any release of personal patron data, the licensee and casino operator shall notify the patron(s) affected in accordance with R.S. 51:3074 and notify the board immediately.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2016 (November 2018).

§2807. Incident Response Plan

A. To ensure that computer systems and network security threats are responded to in a timely and effective manner, an operational incident response plan shall be developed, implemented, and maintained. Licensees and casino operators shall reference the incident response plan in their internal controls, but the plan shall be maintained outside the internal controls to ensure it is updated.

B. The incident response plan shall:

1. detail adequate preparation, detection, analysis, containment, recovery, and response activities;

2. define roles and responsibilities in the event of a security incident;

3. include measures for tracking, documenting, and reporting security incidents to appropriate officials and/or authorities and the division;

4. have a definitive communication plan including both internal and external communication; and

5. be formally documented and tested every three years.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2016 (November 2018).

§2809. Limited Access to Information Systems and Networking Devices

A. A licensee and casino operator shall:

1. ensure that individuals occupying positions with access to sensitive computer hardware, software, or business personnel or patron data including, but not limited to, third-party service providers meet documented security criteria for such positions;

2. ensure that information and information systems remain protected during and after all personnel actions including, but not limited to, terminations and transfers; and

3. implement formal sanctions for the failure of personnel to comply with security policies and procedures.

B. Access to systems, data, and information shall be restricted by job functions. A licensee and casino operator shall establish security groups to ensure that access to computer systems shall be granted to authorized users only and be used solely for the types of transactions and functions that an authorized user is permitted to exercise.

1. A licensee's or casino operator's information technology (IT) department shall review the system access logs at the end of each month. Discrepancies shall be investigated, documented, and maintained for a period of five years.

2. A licensee and casino operator shall maintain personnel access listings that include, at a minimum, the employee's name, position, identification number, and a list of functions the employee is authorized to perform, including the date that authorization is granted. These files shall be updated as employees or the functions they perform change.

3. All changes to the system and the name of the individual who made the change shall be documented.

4. Reports and all other output generated from the system(s) shall only be available and distributed to authorized personnel.

C. All access to the server areas shall be documented on a log maintained by IT. Such logs shall be available at all times. The logs shall contain entries with the following information:

1. name of each person entering the room;

2. reason each person entered the room;

3. date and time each person enters and exits the room;

4. date, time, and type of any equipment malfunction in the room;

5. a description of any unusual events occurring in the room; and

6. such other information required in the internal controls.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2017 (November 2018).

§2811. Protection of Communications

A. A licensee and casino operator shall:

1. monitor, control, and protect all communication and information transmitted or received by the casino's computer systems at the external and internal boundaries of those systems; and

2. employ software development techniques, architectural designs, and systems engineering principles that promote effective information security within the casino's information systems.

B. To the extent possible and practical, all network communications and storage of confidential or sensitive data shall be encrypted. At a minimum, personal patron data shall be considered confidential. Personal patron data shall include, but not be limited to, any non-public patron information collected by the casino, such as date of birth, social security number, credit card number, bank account information, and driver's license number. The importance of additional data may vary as a function of how critical that data is to the integrity of the network and/or the needs of the casino. A licensee and casino operator must assess the type of data that the network carries or stores and determine the relative sensitivity of such information. This assessment shall then serve as a guide to the types of security measures that are appropriate for the network.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2017 (November 2018).

§2813. Training

A. All personnel with access to information systems for any purpose shall be trained to understand how these systems can be compromised by outside agents through personal contact and misrepresentations by those agents as to their identity and need for access to any information concerning the systems or the information they protect. All such attempts by anyone to gain information about information systems including passwords or access should be reported to the person in charge of information security immediately. This training shall be documented.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2017 (November 2018).

§2815. Audit of System and User Activities

A. A licensee and casino operator shall:

1. create, protect, and retain information system audit records to the extent necessary to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and

2. ensure that the actions of individual information system users can be uniquely traced to those users so that

they may be identified and held accountable for their actions.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2017 (November 2018).

§2817. Backup and Recovery

A. IT shall backup system data daily. Backup and recovery procedures shall be written and distributed to all applicable personnel. These policies shall include information and procedures that detail, at a minimum, a description of the system, access to system manuals, and other procedures that ensure the timely restoration of data in order to resume operations after a hardware or software failure.

B. Licensees and the casino operator shall maintain system-generated edit reports, exception reports, and transaction logs.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2018 (November 2018).

§2819. Application Controls

A. Application controls shall include procedures that provide assurance of the accuracy of the data input, the integrity of the processing performed, and the verification and distribution of the output generated by the system. Examples of proper controls include:

1. proper authorization prior to data input, for example, passwords;

2. use of parameters or reasonableness checks; and

3. use of control totals on reports and comparison of them to amounts input.

B. Documents created from the above procedures shall be maintained for a period of five years.

C. Computer Control

1. The delete option within an individual program shall be secured so that only authorized users can execute it. The delete option shall not allow for the deletion of any gaming transaction or void.

2. A licensee and casino operator shall require employees and vendors to change passwords in accordance with documented password security best practices, as specified in the internal controls. Password complexity shall be of sufficient strength to ensure security against false entry by unauthorized personnel.

3. The secured copies, restricted copies, and other electronically stored documents required by these rules and those necessary to calculate gaming revenue and expenses shall be retained for five years.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2018 (November 2018).

§2821. Remote Access Requirements

A. Each licensee and casino operator shall establish and maintain a remote access policy that controls access to the slot monitoring system (SMS), casino management system (CMS), gaming equipment, and other related systems. This includes, but is not limited to, computer controlled key control devices and ticket cashing kiosks. Access shall be controlled from any terminal that is not physically located within or adjacent to the casino property. Write access to gaming systems shall only be provided to gaming permitted employees or controlled on a per access basis by a gaming permitted employee. "Read only" access is not prohibited by this policy. A help desk may remotely login to other user accounts in accordance with corporate IT policies to provide assistance as necessary. The remote access policy shall, at a minimum, contain these requirements:

1. login and transaction security shall be in accordance with a licensee or casino operator's remote access policy;

2. all remote access must be traceable to an authorized individual. There shall be no sharing of accounts or passwords that would result in ambiguity as to which person was involved in any remote access;

3. accounts shall be set up to allow only access to those applications, functions, or accounts necessary. selective access shall be as specific and limited as the operating system or security system will allow;

4. all security related events shall be logged, and any unusual event must be investigated including, but not limited to, failed login attempts and attempts to access restricted assets; and

5. access shall be blocked immediately when it is no longer required by an individual to complete the job function.

B. A record shall be made and kept of any and all changes made and actions taken during each remote access. IT help desk activity shall be in accordance with the company's IT policy and help desk logs (help tickets, help desk activity reports, etc.) shall meet the requirements of this Section. The record shall be clear, comprehensible, and thorough, and shall record all configuration and activity details of remote access connectivity. If remote access activity is related to normal system transactions, audit logs of the transactions will meet the requirement of recording activity. The record shall be reviewed quarterly by appropriate personnel to confirm that the authorized task was completed. Discrepancies shall be investigated.

C. The system access log, change log, security log, and investigation results shall be documented in a way that can be displayed or printed upon request by the board or division and shall be maintained for a period of five years.

D. A backup of system data, gaming data, and software shall be completed prior to remote access if any anticipated action is expected to endanger the system or data. The backup shall contain no less than the previous day's data.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2018 (November 2018).

§2823. Disaster Recovery Plan

A. Licensees and casino operators shall establish a documented contingency plan to mitigate loss or harm and ensure that all critical data is retrievable and that it can be restored to a usable format as quickly and efficiently as possible in the event that a system or service becomes

unavailable. The contingency plan shall be updated regularly and shall remain current with system changes and developments.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2018 (November 2018).

§2825. Computer Monitoring Requirements of Electronic Gaming Devices

A. Each licensee and casino operator shall have a system connected to all EGDs in the casino that are activated for patron play that records and monitors the activities of such devices. No EGDs shall be operated unless it is connected to the system. Licensees and casino operators shall use a system approved by a designated gaming laboratory specified by the division or board. Such system shall provide on-line, real-time monitoring, and data acquisition capabilities.

1. Licensees and casino operators shall immediately report any occurrence of malfunction or interruption of communication between the EGDs and the system to the division. These malfunctions include, but are not limited to, a system down for maintenance or malfunctions, zeroed meters, and invalid meters.

2. Prior written approval from the division is required before implementing any changes to the computerized EGD monitoring system. Licensees and casino operators shall notify the division when transitioning to manual procedures when the EGD monitoring system is down. Changes to the operating system of the EGD monitoring system recommended by the operating system vendor may be made after notification of the operating system upgrade to the division, and do not require prior written approval.

3. Each modification of the application software shall be approved by a designated gaming laboratory specified by the division or board.

B. The system required in Subsection A of this Section shall be designed and operated to automatically perform and report functions relating to EGD meters, and other functions and reports including, but not limited to:

1. record the number and total value of cash equivalents placed in the EGD for the purpose of activating play;

2. record the total value and number of each value of currency and tickets received from the currency acceptor for the purpose of activating play;

3. record the number and total value of cash equivalents deposited in the drop bucket of the EGD;

4. record the number and total value of cash equivalents automatically paid by the EGD as the result of a jackpot;

5. record the number and total value of cash equivalents to be paid manually as the result of a jackpot. The system shall be capable of logging in this data if such data is not directly provided by EGD;

6. have an on-line computer alert and alarm monitoring capability to ensure direct scrutiny of conditions detected and reported by the EGD including any device malfunction, any type of tampering, and any open door to the drop area. Any person opening the EGD or the drop area, except the drop team, shall complete the machine entry authorization log including time, date, machine identity, and reason for entry;

7. be capable of logging in and reporting any revenue transactions not directly monitored by the token meter, including tokens placed in the EGD as a result of a fill and any tokens removed from the EGD in the form of a credit;

8. record date, time, and EGD identification number of any EGD taken off-line or placed on-line; and

9. report the time, date, and location of open doors or events specified in §4201.G.2 of this Part by EGD.

C. All date and time generators shall be based on a synchronized central or master clock.

D. A licensee and casino operator shall store, in machine-readable format, all information required by Subsection B of this Section for a period of five years. A licensee and casino operator shall store all information in a secure area and certify that this information is complete and unaltered. This information shall be available upon request by a division agent in the format and media approved by the division.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 44:2019 (November 2018).

Chapter 42. Electronic Gaming Devices

§4205. Computer Monitoring Requirements of Electronic Gaming Devices

Repealed.

AUTHORITY NOTE: Promulgated in accordance with R.S. 27:15 and 24.

HISTORICAL NOTE: Promulgated by the Department of Public Safety and Corrections, Gaming Control Board, LR 38:1674 (July 2012), repealed LR 44:2019 (November 2018).

Ronnie Jones
Chairman

1811#019

RULE

Department of Public Safety and Corrections Office of MotorVehicles

Administrative Hearing Requests for Suspensions and Disqualifications Arising from Tests for Suspected Drunken Drivers (LAC 55:III.113)

Under the authority of R.S. 32:667(A), and in accordance with the provisions of the Administrative Procedure Act, R.S. 49:950 et seq., the Department of Public Safety and Corrections, Public Safety Services, Office of Motor Vehicles (department), adopts a Rule regarding Administrative Hearing Requests for Suspensions and Disqualifications Arising from Tests for Suspected Drunken Drivers. This notice repeals and overwrites the existing §113 as the duration of a driver's license is address in R.S. 32:412. This §113 is new and implements the provisions of Act 291 of the 2018 Regular Session of the Louisiana Legislature