

**Title 11—DEPARTMENT OF PUBLIC SAFETY
Division 45—Missouri Gaming Commission
Chapter 5—Conduct of Gaming**

PROPOSED AMENDMENT

11 CSR 45-5.237 Shipping of Electronic Gaming Devices, Gaming Equipment or Supplies.
The commission is amending the Purpose statement and section (1).

PURPOSE: This amendment changes requirements for prior approval for shipping gaming equipment and supplies to reflect current procedures.

*PURPOSE: This rule requires licensees to [notify the] **obtain** Missouri Gaming Commission **approval** prior to shipping electronic gaming devices into, out of, or within the state.*

(1) Licensees shipping electronic gaming devices or gaming equipment/supplies as defined in 11 CSR 45-1.090, with the exception of critical program storage media as defined in 11 CSR 45-1.090, into, out of, or within Missouri, must file *[on a form]* **a request in a format** specified by the **Missouri Gaming [c]Commission (MGC) [notice]** at least five (5) days prior to such shipment. **The licensee shall receive MGC approval of the request prior to shipping the listed items.**

*AUTHORITY: section 313.004, RSMo 2000 **and sections** 313.805 and 313.807.4, **RSMo Supp. 2012.** Original rule filed Sept. 2, 1997, effective March 30, 1998. Amended: Filed April 3, 2001, effective Oct. 30, 2001. Amended: Filed Oct. 31, 2005, effective May 30, 2006. Amended: Filed June 19, 2006, effective Feb. 28, 2007. Amended: Filed Oct. 31, 2013.*

PUBLIC COST: This proposed amendment will not cost state agencies or political subdivisions more than five hundred dollars (\$500) in the aggregate.

PRIVATE COST: This proposed amendment will not cost private entities more than five hundred dollars (\$500) in the aggregate.

*NOTICE OF PUBLIC HEARING AND NOTICE TO SUBMIT COMMENTS: Anyone may file a statement in support of or in opposition to this proposed amendment with the Missouri Gaming Commission, PO Box 1847, Jefferson City, MO 65102. To be considered, comments must be received within thirty (30) days after publication of this notice in the **Missouri Register**. A public hearing is scheduled for Wednesday, January 15, 2014, at 10:00 a.m., in the Missouri Gaming Commission's Hearing Room, 3417 Knipp Drive, Jefferson City, Missouri.*

**Title 11 – DEPARTMENT OF PUBLIC SAFETY
Division 45 – Missouri Gaming Commission
Chapter 9 – Internal Control System**

PROPOSED RULE

11 CSR 45-9.111 Minimum Internal Control Standards (MICS)—Chapter K

*PURPOSE: This rule establishes the internal controls for Chapter K of the **Minimum Internal Control Standards**.*

PUBLISHER’S NOTE: The secretary of state has determined that the publication of the entire text of the material which is incorporated by reference as a portion of this rule would be unduly cumbersome or expensive. This material as incorporated by reference in this rule shall be maintained by the agency at its headquarters and shall be made available to the public for inspection and copying at no more than the actual cost of reproduction. This note applies only to the reference material. The entire text of the rule is printed here. The Minimum Internal Control Standards may also be accessed at <http://www.mgc.dps.mo.gov>.

(1) The commission shall adopt and publish minimum standards for internal control procedures that in the commission’s opinion satisfy 11 CSR 45-9.020, as set forth in *Minimum Internal Control Standards* (MICS) Chapter K—Currency Transaction Reporting, which has been incorporated by reference herein, as published by the Missouri Gaming Commission, 3417 Knipp Dr., PO Box 1847, Jefferson City, MO 65102. Chapter K does not incorporate any subsequent amendments or additions as adopted by the commission on October 30, 2013.

AUTHORITY: section 313.004, RSMo 2000, and sections 313.800 and 313.805, RSMo Supp. 2012. Original rule filed Oct. 31, 2013.

PUBLIC COST: This proposed rule will not cost state agencies or political subdivisions more than five hundred dollars (\$500) in the aggregate.

PRIVATE COST: This proposed rule will cost thirteen (13) riverboat casinos sixteen thousand nine hundred dollars (\$16,900) annually in the aggregate. A fiscal note has been filed with this proposed rule.

*NOTICE OF PUBLIC HEARING AND NOTICE TO SUBMIT COMMENTS: Anyone may file a statement in support of or in opposition to this proposed rule with the Missouri Gaming Commission, PO Box 1847, Jefferson City, MO 65102. To be considered, comments must be received within thirty (30) days after publication of this notice in the **Missouri Register**. A public hearing is scheduled for Wednesday, January 15, 2014, at 10:00 a.m., in the Missouri Gaming Commission’s Hearing Room, 3417 Knipp Drive, Jefferson City, Missouri.*

MISSOURI GAMING COMMISSION
MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER K - CURRENCY TRANSACTION REPORTING

CONTENTS

| <u>Section</u> | <u>Page</u> |
|---|-------------|
| § 1. General | K-2 |
| § 2. Logging Cash Transactions In Excess of \$3,000 | K-2 |
| § 3. Reportable Transactions | K-3 |
| § 4. Obtaining and Verifying Identification | K-4 |
| § 5. Circumvention of Currency Transaction Reporting Requirements and Suspicious Activity | K-6 |

Note: Sections 313.800 through 313.850, RSMo., et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class A licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. Revised Oct. 30, 2007. Revised October 30, 2013.

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER K - CURRENCY TRANSACTION REPORTING**

§ 1 **General**

- 1.01 Each Class B Licensee shall ensure that the minimum reporting requirements for Currency Transaction Reports (CTR) are satisfied.

- 1.02 Each Class B Licensee shall designate in the internal controls the job title of the specific person (CTR Compliance Officer) responsible for the day-to-day compliance with the CTR requirements.

- 1.03 Each Class B Licensee will be responsible for developing a training program for casino personnel on compliance with the CTR requirements.

- 1.04 Compliance with the MICS does not release the Class B Licensee from its obligation to comply with all applicable state and federal regulations.

- 1.05 Systems for tracking currency transactions, such as automated tracking, shall be described in the internal controls.

- 1.06 The cash transactions referred to in this chapter include, but are not limited to:
 - (A) Cash In:
 - (1) safekeeping deposits;
 - (2) purchase of a casino check by a patron;
 - (3) purchase of chips;
 - (4) exchange of currency for currency, including foreign currency;
 - (5) bills inserted in EGDs, if identifiable to a patron and available from the system; and
 - (6) any other transaction where cash comes from the patron to the cage.

 - (B) Cash Out:
 - (1) chip redemptions;
 - (2) payment of winnings, except slot jackpots;
 - (3) safekeeping withdrawals;
 - (4) cashing checks;
 - (5) exchange of currency for currency, including foreign currency;
 - (6) EGD tickets redeemed at the cage;
 - (7) EGD tickets inserted in kiosks, if identifiable to a patron and available from the system; and
 - (8) credit meter payouts.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class A licensees should review these statutes and rules to ensure their internal controls includes compliance with the requirements set forth. Revised Oct. 30, 2007. Revised October 30, 2013.

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER K - CURRENCY TRANSACTION REPORTING**

§ 2 Logging Cash Transactions In Excess of \$3,000

- 2.01 Single cash transactions, as identified in section 1 of this chapter, in excess of \$3,000 and known aggregate transactions in the same directional flow that exceed \$3,000 must be logged in the appropriate department's multiple transaction log (MTL). These logs shall cover the entire gaming day.
- 2.02 The internal controls shall indicate which departments maintain multiple transaction logs. If a computerized log is shared by departments, the internal controls shall indicate which departments share the log.
- 2.03 Once a patron's known aggregate cash activity in the same directional flow has exceeded \$3,000, all additional cash transactions identifiable to the patron of \$500 or more must be logged regardless of location.
- 2.04 The employee conducting a single cash transaction in excess of \$3,000 with a patron is responsible for ensuring the transaction is recorded on the multiple transaction log. The employee is not personally required to complete the log, but must verify that the entry is completed. Transactions under \$3,000 which must be logged because the patron's aggregate cash activity exceeded \$3,000 in the same directional flow shall be logged by the employee who has knowledge of the aggregate cash activity. If the transactions are not discovered until the compilation process, the transactions shall be logged by the individual performing the process.
- 2.05 Employees required to record MTL entries shall review the multiple transaction logs at the beginning of their shift to familiarize themselves with the cash activity that occurred during the previous shift(s) that gaming day.
- 2.06 If manual logs are used, the completed multiple transaction logs shall be submitted to the appropriate audit department on a daily basis. If no activity occurs on the log for a given department, this shall be indicated on the log that is submitted.
- 2.07 If a patron refuses to provide his/her name for a cash transaction, such refusal shall be documented on the MTL by the employee.

§ 3 Reportable Transactions

- 3.01 All cash transactions in excess of \$10,000 must be reported on a CTR. This includes any single transaction or series of related multiple transactions conducted by, or on behalf of the same patron, with the same directional flow within the same gaming day.
- 3.02 The employee conducting the transaction which triggered the requirement for a CTR is responsible for obtaining all the required information for the proper completion of the

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class A licensees should review these statutes and rules to ensure their internal controls includes compliance with the requirements set forth. Revised Oct. 30, 2007. Revised October 30, 2013.

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER K - CURRENCY TRANSACTION REPORTING**

CTR. The CTR shall be prepared by the individual conducting the transaction or by an individual(s) whose job title is specified in the internal controls as being designated to perform this duty. When the need for a CTR is not able to be determined until additional information regarding cash transactions for that patron, which was not available to the employee on the gaming floor, was compiled after the end of the gaming day, the CTR shall be prepared by the individual performing the compilation process or by an individual whose job title is specified in the internal controls as being designated to perform this duty.

- 3.03 All CTRs must be properly filed with the Financial Crimes Enforcement Network (FinCEN) by the 15th day after the date of the transaction. The submission confirmation documentation shall be maintained. At the time of submission an electronic copy of each CTR shall be submitted to the MGC Boat Sergeant.

§ 4 Obtaining and Verifying Identification

- 4.01 Prior to concluding a single cash transaction in excess of \$10,000 or any other transaction which causes the patron's total cash in or cash out to exceed \$10,000, the following patron identification information shall be obtained:
- (A) patron's last name, first name, and (if provided) middle initial;
 - (B) patron's full address, including number and street, city, state, zip code, and country if other than United States;
 - (C) patron's social security number;
 - (D) patron's date of birth;
 - (E) passport number or alien identification number and issuing country if a patron is an alien or non-resident of the United States, if presented; and
 - (F) type of identification used to verify the above information, including the identification number and state/country of issuance.
- 4.02 If an individual (agent) is conducting a transaction on behalf of another individual, the same identification information as required for the patron conducting the transaction must be obtained for the person serving as the agent. This is in addition to the information required for the individual for whom the transaction is being conducted.
- 4.03 All identification information must be verified by examining the identification presented by the patron. For a patron for whom a safekeeping deposit has been accepted with proper identification, check cashing authority has been granted, or for whom a CTR containing verified identity has been filed, acceptable identification information obtained previously and maintained in the Class B Licensee's internal records may be used, as long as the following conditions are met:
- (A) the patron's identity is re-verified at least every two years;

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class A licensees should review these statutes and rules to ensure their internal controls includes compliance with the requirements set forth. Revised Oct. 30, 2007. Revised October 30, 2013.

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER K - CURRENCY TRANSACTION REPORTING

- (B) any out-of-date identifying information is updated in the internal records;
 - (C) the date of each re-verification is noted in the internal records; and
 - (D) the identification has not expired.
- 4.04 Acceptable identification for U.S. residents includes valid, non-expired:
- (A) driver's license. The photo requirement may be waived on the license if issued by jurisdictions not requiring a photo;
 - (B) U.S. passport;
 - (C) other state-issued photo I.D. cards. The photo requirement may be waived on identification issued by jurisdictions not requiring a photo;
 - (D) military identification card or military dependent card; or
 - (E) other form of picture ID with either a social security card or a birth certificate.
- 4.05 Acceptable identification for aliens or non-residents includes valid, non-expired:
- (A) Passport;
 - (B) Alien registration card; or
 - (C) Other official documents evidencing nationality or residence (e.g., Provincial Driver's License).
- 4.06 If the need for a CTR is not determined until the end of the day compilation process, the individual's identification information may be obtained from existing records, if available.
- 4.07 For each CTR, a clear copy of the photo identification used to verify the patron's identity (either the one in the system or the one presented) shall be kept on file with the CTR. If a clear copy of photo identification is not available, Surveillance shall be notified prior to the completion of the qualifying transaction and the surveillance employee shall obtain at least one photograph of the patron from the surveillance camera. The surveillance photo of the patron shall be kept on file with the CTR. The photograph or the image file shall be labeled with the patron's name. If the need for a CTR is not determined until the end of the day compilation process has occurred, a photo or a copy of the patron's identification from existing records may be used even if the identification is expired.
- 4.08 If the patron is unable to provide any of the above information or the identification provided is not acceptable, the transaction must be refused until the necessary information has been obtained.
- 4.09 If a patron refuses to provide proper identification, all cash transactions shall be stopped and the patron shall be barred from any further gaming activity until adequate identification is provided.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class A licensees should review these statutes and rules to ensure their internal controls includes compliance with the requirements set forth. Revised Oct. 30, 2007. Revised October 30, 2013.

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER K - CURRENCY TRANSACTION REPORTING**

- 4.10 If the denied transaction involves chip redemptions and the patron is unable to provide adequate identification, the patron has the option of keeping the chips or placing them on deposit. If the denied transaction involves the payment of winnings and the patron is unable to provide adequate identification, the casino shall place the winnings in safekeeping until adequate identification is provided.

§ 5 Circumvention of CTR Requirements and Suspicious Activity

- 5.01 A Suspicious Activity Report (SAR) shall be prepared for any transaction(s) or attempted transaction(s) if it is conducted or attempted by, at, or through a casino and involves or aggregates at least \$5,000 in funds or other assets and the casino knows, suspects or has reason to suspect that the transaction or series of transactions involves funds derived from illegal activity or are being structured to avoid federal transaction reporting requirements. If the transaction or series of transactions also result in an aggregate cash-in or cash-out of more than \$10,000 a CTR must also be prepared and filed.
- 5.02 The SAR shall be filed within 30 days after the casino becomes aware of the suspicious transaction. If the casino is unable to identify the suspect on the date the transaction is initially detected, the casino has an additional 30 days to identify the suspect before filing the SAR, but the suspicious transaction must be reported within 60 calendar days after the date of the initial detection of the suspicious transaction, whether or not the casino is able to identify the suspect. At the time of submission an electronic copy of each SAR shall be submitted to the MGC Boat Sergeant.
- 5.03 Employees are responsible for preventing a patron from circumventing the CTR reporting requirements if the employee has knowledge, or through reasonable diligence in performing their duties should have knowledge, of the patron's attempt. Employees shall not provide any information to anyone to assist in the circumvention of CTR reporting requirements.
- 5.04 If a patron requests currency and upon being informed of the CTR reporting requirements, requests a check or a portion of the transaction being both check and currency, or pulls back chips so there is less than \$10,000 cash involved, the transaction shall be handled as a suspicious transaction and all appropriate procedures shall be followed.
- 5.05 If a patron refuses to provide any identification, all currency transactions shall be terminated and the patron shall be barred from any further gaming activity until all the necessary information has been properly provided. Surveillance and Security shall be notified. A picture of the patron shall be taken by Surveillance, and Surveillance shall monitor and record Security escorting the patron from the gaming area. The patron shall not be allowed to return until all necessary information has been provided. The MGC

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class A licensees should review these statutes and rules to ensure their internal controls includes compliance with the requirements set forth. Revised Oct. 30, 2007. Revised October 30, 2013.

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER K - CURRENCY TRANSACTION REPORTING

agent on duty shall be notified immediately that a patron refused to give the required information, or is attempting to circumvent the reporting requirements and is being escorted from the gaming area. A copy of the recording and picture of the patron shall be supplied to the MGC agent on duty.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class A licensees should review these statutes and rules to ensure their internal controls includes compliance with the requirements set forth. Revised Oct. 30, 2007. Revised October 30, 2013.

**FISCAL NOTE
PRIVATE COST**

**I. TITLE 11 - DEPARTMENT OF PUBLIC SAFETY
Division 45 – Missouri Gaming Commission
Chapter 9 – Internal Control System**

| | |
|-------------------------------|---|
| Rule Number and Title: | 11 CSR 45-9.111 Minimum Internal Control Standards (MICS)— Chapter K |
| Type of Rulemaking: | Proposed Rule |

II. SUMMARY OF FISCAL IMPACT

| Estimate of the number of entities by class which would likely be affected by the adoption of the rule: | Classification by types of the business entities which would likely be affected: | Estimate in the aggregate as to the cost of compliance with the rule by the affected entities: |
|---|--|--|
| 13 | Riverboat Casinos | \$16,900 (annually) |

III. WORKSHEET

The estimated annual cost has been quantified at 13 hours a week (1 hour per casino) at an hourly rate of \$25 (wages + benefits).

$$13 \times 52 \text{ weeks} \times \$25 = \$16,900$$

IV. ASSUMPTIONS

The current standards in MICS K §3.04 and K§ 5.02 require Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) to be filed by the casinos with the Financial Crimes Enforcement Network (FinCEN). The new standards will require the casino to provide an electronic copy of this report to the Boat Sergeant.

This will result in an additional cost to the casinos for the staff time to email the CTRs and SARs to the Boat Sergeants.

The anticipated total cost for this rule will recur annually for the life of the rule.

**Title 11 – DEPARTMENT OF PUBLIC SAFETY
Division 45 – Missouri Gaming Commission
Chapter 9 – Internal Control System**

PROPOSED AMENDMENT

11 CSR 45-9.119 Minimum Internal Control Standards (MICS)—Chapter S. The commission is amending section (1).

PURPOSE: This amendment updates minimum internal control standards to remove the extension date for compliance that was originally granted in 2011. All requirements shall be in place by June 30, 2014. This amendment also clarifies the definition of critical information technology systems and equipment.

PUBLISHER’S NOTE: The secretary of state has determined that the publication of the entire text of the material which is incorporated by reference as a portion of this amendment would be unduly cumbersome or expensive. This material as incorporated by reference in this amendment shall be maintained by the agency at its headquarters and shall be made available to the public for inspection and copying at no more than the actual cost of reproduction. This note applies only to the reference material. The entire text of the amendment is printed here. The Minimum Internal Control Standards may also be accessed at <http://www.mgc.dps.mo.gov>.

(1) The commission shall adopt and publish minimum standards for internal control procedures that in the commission’s opinion satisfy 11 CSR 45-9.020, as set forth in Minimum Internal Control Standards (MICS) Chapter S—Management Information Systems, which has been incorporated by reference herein, as published by the Missouri Gaming Commission, 3417 Knipp Dr., PO Box 1847, Jefferson City, MO 65102. Chapter S does not incorporate any subsequent amendments or additions as adopted by the commission on *[February 23, 2011]* **October 30, 2013**.

AUTHORITY: section 313.004, RSMo 2000 and sections 313.800 and 313.805, RSMo Supp. [2010] **2012**. Original rule filed Oct. 22, 2010, effective June 30, 2011. Amended: Filed Oct. 31, 2013.

PUBLIC COST: This proposed amendment will not cost state agencies or political subdivisions more than five hundred dollars (\$500) in the aggregate.

PRIVATE COST: This proposed amendment will not cost private entities more than five hundred dollars (\$500) in the aggregate.

NOTICE OF PUBLIC HEARING AND NOTICE TO SUBMIT COMMENTS: Anyone may file a statement in support of or in opposition to this proposed amendment with the Missouri Gaming Commission, PO Box 1847, Jefferson City, MO 65102. To be considered, comments must be received within thirty (30) days after publication of this notice in the **Missouri Register**. A public hearing is scheduled for Wednesday, January 15, 2014, at 10:00 a.m., in the Missouri Gaming Commission’s Hearing Room, 3417 Knipp Drive, Jefferson City, Missouri.

MISSOURI GAMING COMMISSION
MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S – MANAGEMENT INFORMATION SYSTEMS (MIS)

CONTENTS

| <u>Section</u> | <u>Page</u> |
|---|-------------|
| § 1. Definitions | S-2 |
| § 2. General | S-4 |
| § 3. Physical Access and Maintenance Controls | S-5 |
| § 4. Critical IT System Parameters | S-5 |
| § 5. User Accounts | S-7 |
| § 6. Generic Accounts | S-8 |
| § 7. Service & Default Accounts | S-9 |
| § 8. Critical IT System Backups | S-10 |
| § 9. Recordkeeping | S-10 |
| § 10. Network Security | S-11 |
| § 11. Changes to Production Environment | S-12 |
| § 12. Remote Access | S-12 |
| § 13. In-House Software Development | S-13 |
| § 14. Purchased Software Programs | S-13 |
| § 15. Wireless Networks | S-14 |
| § 16. Compliance Assessments | S-15 |
| § 17. Player Tracking Systems | S-15 |

*Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).*S-1

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS**

§ 1 Definitions

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

- 1.01 “Administrative access” means access that would allow a user to:
- (A) add, change, or delete system accounts and associated user provisioning;
 - (B) modify operating system, database, and application security and policy parameters;
 - (C) add, change, or delete system exception logging information; and
 - (D) add, change, or delete permissions to data files and folders.
- 1.02 “Backup system log” is an event log, a job log or an activity file created by the program or batch process that performs backups of application and data files. These event logs, job logs or activity files provide detail on the type of backup performed, success or failure of the operation, and a list of errors.
- 1.03 “Character classes” are groups in which standard ASCII characters are defined. There are four character classes:
- (A) lower case alphabetic (i.e., a–z);
 - (B) upper case alphabetic (i.e., A–Z);
 - (C) numeric (i.e. 0–9); and
 - (D) special characters (i.e. ~!@#%&*()_+=-`[]{}|;:'",./<>?).
- 1.04 “Component(s)”: Any network hardware, server(s), Slot Machine Interface Board (SMIB) or application included in, or critical to the operation of the Critical IT System.
- 1.05 “Critical Information Technology (IT) Systems and equipment” includes all components of systems hardware and software, application software (e.g., slot accounting systems, bonusing systems, server supported game systems, cashless systems), and database software that individually or in combination are used for gaming operations. The term does not include user terminals, player tracking systems if independent of the slot accounting system, or electronic gaming devices.
- 1.06 “Default accounts” are accounts created by the manufacturer with predefined access levels which are created by default at installation for operating systems, databases, and applications. This also includes accounts with full system access (e.g., “Administrator,” “root,” and “sa”) regardless if their names have been changed.
- 1.07 “Generic accounts” are accounts shared by multiple users (using the same password) with access to Critical IT Systems and equipment and applications.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS

- 1.08 “Group membership” (group profile) is a method of organizing user accounts into a single unit (by job authority) whereby access to application functions may be modified at the unit level and the changes take effect for all user accounts assigned to the unit.
- 1.09 “Local intranet” is a network which only includes the Class B Licensee’s local facility.
- 1.10 “Management Information Systems (MIS) personnel” are employees that have been designated in the Internal Control System to perform the information technology function for the operation of Critical IT Systems and equipment.
- 1.11 “National Institute of Standards and Technology” (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce.
- 1.12 “Remote access” refers to connectivity to the Class B licensee’s internal network from employees and vendors originating from sources outside the Class A or B licensee’s private network.
- 1.13 “Security incident” is any occurrence that jeopardizes the confidentiality, integrity, or availability of a Critical IT System or the information the system processes, stores, or transmits or that constitutes a violation of the Internal Control System or MGC rules and regulations.
- 1.14 “Service accounts” are accounts on which automated system functions are dependent to execute. These accounts provide a certain level of access necessary for normal operation of applications and/or automated batch processes.
- 1.15 “Slot accounting system” is an on-line monitoring and control system that continuously monitors each EGD via a defined communication protocol by either: a dedicated line, dial up system, or other secure transmission method. The system’s primary task is to provide logging, searching and reporting of gaming significant events, collection of individual device financial and meter data, reconciliation of meter data against soft counts and system security.
- 1.16 “System administrator” is the individual(s) responsible for maintaining the stable operation of the MIS environment (including software and hardware infrastructure and application software).
- 1.17 “Third party software developer” is any software developer other than Class A or Class B licensees.
- 1.18 “Threat analysis” is the examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS**

- 1.19 “User accounts” are all accounts other than default accounts, generic accounts or service accounts.
- 1.20 “Vulnerability” is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited and result in a security breach or a violation of the system security policy.
- 1.21 “Wireless network components” include all hardware, software and encryption mechanisms which are involved in IEEE 802.11 wireless networks and the licensee’s wireless environment. This includes, at a minimum:
- (A) supplicants;
 - (B) authenticators (e.g., access points, controllers, etc.);
 - (C) authentication servers (i.e., RADIUS servers);
 - (D) AES/CCMP; and
 - (E) EAP Methods (e.g., EAP/TLS).

§ 2 General

- 2.01 Unless otherwise specified, all Management Information Systems (MIS) MICS apply to Critical IT Systems as defined in MICS Chapter S.
- 2.02 The MIS department shall be independent of all other departments. MIS personnel shall not perform the duties of other departments.
- 2.03 MIS personnel shall not have signatory ability on gaming documents that affect Adjusted Gross Receipts (e.g., slot jackpot forms, table games fill/credit forms, etc.).
- 2.04 Class B Licensees shall not outsource MIS department functions relating to Critical IT Systems and equipment to unlicensed individuals or entities unless otherwise approved in writing by MGC.
- 2.05 At least one MGC licensed MIS employee shall be on call 24 hours a day.
- 2.06 All Critical IT System accounts shall be one of the following:
- (A) generic account;
 - (B) default account;
 - (C) service account; or
 - (D) user account.
- 2.07 Each individual who has write capability to Critical IT Systems, including remote access, shall possess an MGC occupational license, unless otherwise approved in writing by MGC.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS**

§ 3 Physical Access and Maintenance Controls

- 3.01 Access to areas (i.e., rooms, cabinets, racks, etc.) housing Critical IT Systems and equipment shall be locked and access restricted to MGC licensed MIS personnel with the use of a sensitive key/proximity card. All non-MIS personnel shall be escorted by a licensed MIS employee while accessing areas housing Critical IT Systems and equipment with the exception of areas that solely house slot accounting systems or server supported game systems which may be accessed by slot technicians, or above within the slot department.
- 3.02 The Critical IT Systems servers shall reside in a secure room(s) which shall:
- (A) have surveillance coverage that permits identification of anyone accessing the room and accessing any Critical IT Systems servers;
 - (B) utilize uninterruptible power supply; and
 - (C) be equipped with fireproof and waterproof materials to protect critical hardware from natural disaster (e.g., FM-200), which meet local fire laws and regulations.
- 3.03 If an individual who has access to the secured Critical IT Systems and equipment is suspended subject to termination, terminated or transferred to another department, the individual's access shall be terminated within 72 hours of the change in status.
- 3.04 Unprovisioned network jacks shall be designed to deny access to Critical IT Systems either physically or logically. The network jacks shall only be opened when access is required.
- 3.05 All communication closets (e.g., wiring closets) shall be locked when not occupied and shall have dedicated surveillance coverage.

§ 4 Critical IT System Parameters

- 4.01 The Critical IT Systems shall be logically secured through the use of passwords, biometrics, or other means approved in the Internal Control System.
- 4.02 All passwords shall be encrypted during electronic transmission and storage on all Critical IT Systems.
- 4.03 Security parameters for passwords shall meet the following minimum requirements. These requirements apply to all accounts except for service accounts and generic accounts.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS

- (A) Passwords shall expire at least every 90 days.
 - (B) Passwords shall be at least eight characters comprised of three of the four character classes.
 - (C) Passwords shall not be reused for a period of 18 months or be reused within the last ten password changes.
 - (D) Passwords shall be confidential.
 - (E) Accounts shall be automatically locked out after three failed login attempts. The system may release a locked out account after 30 minutes have elapsed.
- 4.04 Administrative access to the network, operating system, applications, and database security and system parameters shall be limited to MIS personnel, both local and corporate, unless otherwise approved in writing by MGC.
- 4.05 The Class B Licensee shall maintain a daily system event log for Critical IT Systems which shall track the following:
- (A) security incidents as described in a submission to the MGC;
 - (B) changes to the policies and parameters of the operating system, database, and network;
 - (C) audit trail of information changed by administrator accounts; and
 - (D) changes to date/time on master time server.
- 4.06 Daily system event logs shall be reviewed at least once a week for each day of the entire previous calendar week for the events listed above. The system event logs shall be maintained for a minimum of one year. This review may either be completed manually by MIS personnel or by using an automated tool that polls the event logs for all gaming related servers and provides the system administrators notification. The Internal Control System shall indicate how this review will be completed. Evidence of this review (e.g., log, checklist, notation on reports) shall include:
- (A) date;
 - (B) time;
 - (C) name of individual performing the review (if a manual review);
 - (D) exceptions noted; and
 - (E) any follow-up of the noted exception.
- 4.07 All security incidents or malfunctions that affect the availability of the system shall be reported to the MGC agent on duty.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS**

- 4.08 The Critical IT Systems shall log out or lock the screen of all currently logged in user sessions, other than accounts with read-only access, after 15 minutes of inactivity.
- 4.09 Prior to the implementation of any new Critical IT System, the MGC may require a third-party to review the topology layout, rapid recovery strategies and failover procedures.
- 4.10 All Critical IT Systems shall employ network-based time synchronization (e.g., network time protocol).
- 4.11 Personal identification numbers (PINs) shall be encrypted during electronic transmission and storage on all Critical IT Systems. During storage, PINs shall be encrypted with at least a 128-bit key size.

§ 5 User Accounts

- 5.01 Each user account shall be assigned to an individual and shall not be made available to or used by any other individual. The individual assigned to the user account will be held responsible for all activities performed under that individual's user account.
- 5.02 A system administrator shall establish all user accounts. Each account shall only provide access consistent with the employee's current job responsibilities as delineated in the employee's job description. The access shall maintain a proper segregation of duties and restrict unauthorized users from viewing, changing or deleting critical files and directories. The user accounts established for MIS personnel must be reviewed and approved by the MIS Manager. The approval must be documented.
- 5.03 Anytime an employee transfers to a new position, the employee's accounts shall be disabled within 72 hours of the change in position and prior to the assignment of any new access required by the employee's new position. Provisioning of users' accounts consists of assigning application functions matching the employee's current job responsibilities to ensure adequate separation of duties. Provisioning of user accounts for employees who transfer to a new department shall be reviewed and approved by management personnel. Any previously assigned application function access for the employee's user account is changed to inactive (disabled) prior to the employee accessing his/her new user account for his/her role or position in a new department.
- 5.04 The Class B Licensee shall generate on request user access listings, which shall include at a minimum:
 - (A) employee name;
 - (B) title or position;
 - (C) user login name;
 - (D) full list and description of application functions that each group/user account may execute;

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS**

- (E) date and time account created;
- (F) date and time of last login;
- (G) date of last password change, if configurable;
- (H) date and time account disabled/deactivated/reactivated; and
- (I) group membership of user account, if applicable.

- 5.05 When multiple user accounts for one employee per application are used, only one user account shall be active (enabled) at a time, if the concurrent use of the multiple accounts by the employee could create a segregation of duties deficiency. Additionally, the user account shall have a unique prefix/suffix to easily identify the users with multiple user accounts within one application.
- 5.06 The MIS department shall be notified upon termination of any employee. The terminated employee's user account(s) shall be disabled or deactivated within 72 hours of termination or suspension subject to termination; or if the user account has remote access, the account shall be disabled by the end of the next gaming day.

§ 6 Generic Accounts

- 6.01 Generic accounts shall be restricted to read-only access.
- 6.02 Generic accounts at the operating system level, if used, shall be configured such that the user is automatically brought to the application logon screen immediately upon logging into the operating system. The generic accounts shall also be configured such that the user is logged out of the operating system automatically upon exiting the application.
- 6.03 Generic accounts shall be unique to each application. Generic accounts cannot exist across multiple applications.
- 6.04 The Class B Licensee shall identify in a submission to the MGC the generic accounts and the generic accounts' permissions that will be used to access Critical IT Systems.
- 6.05 A system administrator shall establish all generic accounts. Each account shall only provide access consistent with the generic users' current job responsibilities as specified in the job descriptions for the generic users.

§ 7 Service & Default Accounts

- 7.01 Service accounts, if used, shall be utilized in a manner to prevent unauthorized and inappropriate usage. The Internal Control System shall specify the method used to prevent unauthorized and inappropriate usage of all service accounts for each Critical IT System. The method used for each Critical IT System shall either include:

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS**

- (A) configuring the accounts such that the accounts cannot be used to directly log into a Critical IT System; or
 - (B) requiring service account passwords to be changed at least once every 90 days, and by the end of the next gaming day upon termination of any individual with the ability to modify service accounts.
- 7.02 All default accounts shall be disabled prior to system implementation unless they are necessary for proper operation of the system. If these accounts must remain enabled due to system design or limitations, the passwords shall be changed prior to system implementation. Default accounts or any other accounts that have full access over the system or application (e.g., “Administrator,” “root,” and “sa”) shall:
- (A) have passwords that are at least 14 characters long, or at least the maximum system capability if the system is not capable of supporting 14 character passwords;
 - (B) have passwords which contain at least three of the four character classes;
 - (C) not be used unless individual accounts cannot be used (e.g., network failure, or individual administrator accounts are not supported by the system); and
 - (D) have passwords which are changed every 90 days and by the end of the next gaming day upon termination of any individual with the ability to access the account.
- 7.03 Applications must be designed in such a way that passwords are not stored within the application source code. This excludes web applications where application code is stored on a remote server where access to that source code is controlled. If absolutely necessary, credentials may be stored within configuration files (e.g., the Windows registry), but must be stored in such a way that they cannot be accessed or altered without proper authorization.

§ 8 Critical IT System Backups

- 8.01 Daily backup and recovery procedures shall be in place. The backup for all systems shall include:
- (A) application data, if data files have been updated;
 - (B) application executable files (unless such files can be reinstalled); and
 - (C) database contents and transaction logs.
- 8.02 Upon completion of the backup process, the backup media shall be transferred within 72 hours or by the end of the next business day following a federal holiday to an off-site location separate from the location housing the servers and data being backed up for

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS

storage. The storage location shall be secured to prevent unauthorized access and shall provide protection to prevent the permanent loss of data in the event of a fire or other disaster.

- 8.03 Backup system logs shall be reviewed daily by MIS personnel or individuals authorized by MIS personnel to ensure that backup jobs execute correctly and on schedule. The backup system logs shall be maintained for the most recent 30 days.
- 8.04 Class B Licensees shall test data redundancy procedures to ensure data is retrievable at least monthly. Documentation of the test shall be retained.
- 8.05 The backup processes and procedures implemented for restoring data and application files shall be available upon request. The job position of the employee responsible for the backup shall be included in the Internal Control System.

§ 9 Recordkeeping

- 9.01 Critical IT System documentation for all in-use versions of applications, databases, network hardware, and operating systems shall be maintained, including descriptions of both network hardware (including model numbers) and software (including version numbers).
- 9.02 System administrators shall maintain a current list of all enabled generic, service and default accounts. The documentation shall include, at a minimum, the following:
 - (A) name of Critical IT System (i.e., the application, operating system, or database);
 - (B) the account login name;
 - (C) a description of the account's purpose; and
 - (D) a record (or reference to a record) of the authorization for the account.
- 9.03 The current list of all enabled generic, service and default accounts shall be reviewed by MIS management, in addition to the system administrator, at least once every six months to identify any unauthorized or outdated accounts. The review shall be documented. The documentation shall include the list reviewed and supporting evidence of the review.
- 9.04 A current list of all user accounts including the employee's name and the individual's corresponding user provisioning access for all Critical IT Systems and equipment shall be retained for at least one day of each month for the most recent five years. The lists may be archived electronically, if the listing is written to unalterable media (secured to prevent alteration).
- 9.05 The MIS department shall maintain current documentation for all Critical IT Systems used in Missouri or accessed from Missouri with respect to the network topology (e.g., flowchart/diagram), deployment of servers housing applications and databases,

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS**

encryption algorithms, and inventory of software and hardware deployed. The job position(s) responsible for maintaining the current documentation on the network topology shall be delineated in the Internal Control System.

§ 10 Network Security

- 10.01 If guest networks are offered that provide Internet access for patrons, hotel guests, or vendors, they shall be physically or logically segregated from the network used to serve access to any Critical IT Systems and equipment. Traffic on guest networks shall be non-routable to the Critical IT Systems and equipment.
- 10.02 Production networks (live networks) serving Critical IT Systems and equipment shall be secured from outside traffic (e.g., firewall and routers) such that systems are configured to detect and report security related events that could directly affect the integrity of any Critical IT System and equipment. All unused ports, protocols and any unauthorized inbound connections originating from outside the network shall be blocked. The procedures for detecting and reporting security related events shall be documented. The department responsible for the maintenance of the documentation shall be included in the Internal Control System.
- 10.03 Firewall or other equipment used to secure the network from outside traffic shall maintain a 30-day audit log. The audit log shall record all changes to the configuration of the firewall or other equipment, and shall be reviewed weekly for unauthorized configuration changes. The review shall be documented.
- 10.04 An encryption algorithm with a minimum of a 128-bit key size shall be utilized when transmitting or receiving Critical IT System data to or from any source outside of the local intranet.
- 10.05 An automated integrity check mechanism for Critical IT System files and directories deemed critical by a licensed independent testing laboratory shall be deployed at least every 24 hours to monitor unauthorized modifications or corruption.
- 10.06 If configurable, Critical IT Systems and equipment shall utilize virus protection mechanisms to preserve the integrity and operability of the system. The virus protection mechanism(s) shall be updated at least once every 30 days to ensure the protection against known threats.

§ 11 Changes to Production Environment

- 11.01 The process for managing changes to the production environment in a Critical IT System shall be documented. The department responsible for the maintenance of the documentation shall be included in the Internal Control System.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

**MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS**

§ 12 Remote Access

- 12.01 All remote access connections to the Critical IT System(s) shall be granted/authorized through the use of Two-Factor Authentication (T-FA).
- 12.02 Remote access to any Critical IT Systems and equipment shall be monitored by an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS).
- 12.03 For each Critical IT System that can be accessed remotely, the Internal Control System shall specifically address remote access procedures and shall include, at a minimum:
- (A) the method and procedures used in establishing user accounts and passwords to allow authorized vendor personnel to access the system through remote access; and
 - (B) the personnel involved and procedures performed to enable the method of establishing remote access connection to the system when the vendor requires access to the system through remote access.
- 12.04 Vendor remote access shall require:
- (A) Each remote access to a Critical IT System application shall only be granted by a Class A or Class B licensed MIS employee and shall be documented on the Remote Access Log which shall be submitted to the MGC EGD Department by the 10th day of each month;
 - (B) Whenever the remote access connection is not in use it shall be physically or logically disabled to prevent access. Remote access shall be enabled only when approved by a Class A or Class B licensed MIS employee;
 - (C) User accounts required to establish remote access to remain disabled on all operating systems, databases, network devices, and applications until needed. Subsequent to an authorized use by a vendor, the account shall be returned to a disabled state immediately; and
 - (D) The Critical IT System or the operating system to automatically monitor and record the user account name, time and date the connection was made, duration of the connection, and activity while connected, including the specific areas accessed and changes made.

§ 13 In-House Software Development

- 13.01 If source code for Critical IT Systems and equipment is developed or modified internally, a process shall be adopted to manage the development. The Internal Control System shall list the job title of any employee who develops or modifies source code. The process shall include:

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS

- (A) Requests for new programs or program changes shall be reviewed and approved by the MIS supervisory personnel. The review and approval shall be documented by the reviewing MIS supervisory personnel. If software has write privileges into any Critical IT System, it shall be submitted to an MGC licensed testing laboratory for approval; and
- (B) Physical or logical segregation of the development and testing from the production environments.

13.02 Ensure there is a proper segregation of duties such that the individual who develops code shall not be the same individual who conducts the final testing and approves the code. Those individuals who develop or approve the code shall not have access to introduce new or modified code into the production environment.

§ 14 Purchased Software Programs

14.01 Any third party software application that is a Critical IT System or has read or write privileges into any Critical IT System shall be submitted to an MGC licensed testing laboratory. All applications with write privileges shall require a testing laboratory certification letter. Any application with read-only privileges shall require an attestation letter stating the software functions as designed and cannot write to a Critical IT System. All software developers who develop programs with write privileges to Critical IT Systems shall possess an MGC-issued supplier license.

14.02 A System Upgrade Form (SUF), available on the MGC website, shall be submitted prior to the installation of any third party software application that has write privileges into any Critical IT System.

14.03 Testing of new and modified programs shall be performed by the Class A or Class B Licensee or the Critical IT System manufacturer and shall be documented prior to full implementation.

§ 15 Wireless Networks

15.01 Wireless networks used in conjunction with any Critical IT Systems and equipment shall meet the following minimum standards:

- (A) Wireless networks must implement authentication and encryption to ensure all wireless stations are authorized to be on the wireless network and all data packets transmitted on the wireless network are encrypted before being transmitted. Wireless network components must use and implement cryptographic modules and algorithms which comply with the Federal Information Protection Standard 140-2, et seq. (FIPS 140-2), unless otherwise approved in writing by MGC. The Class B Licensee shall maintain all FIPS certificates;

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS

- (B) Wireless client operating systems shall be hardened to provide adequate security in accordance with guidelines released by the NIST's Computer Security Resource Center (CSRC) that most appropriately fit the licensee's environment. For operating systems that are not addressed in the NIST CSRC guidelines, the licensee may instead harden wireless client operating systems in accordance with Security Technical Implementation Guides (STIGs) released by the Defense Information Systems Agency (DISA);
- (C) The wireless network, at a minimum, shall utilize the IEEE 802.11i standard with IEEE 802.1x authentication. Acceptable Extensible Authentication Protocol (EAP) methods must involve Transport Layer Security (TLS) certificate-based mutual authentication. No communication can take place prior to successful authentication between the supplicant and the authentication server. Should a vulnerability be found in the present protocol, MGC reserves the right to require a licensee to adopt the latest non-vulnerable wireless security standards. Any breach to the security of the approved encryption algorithm shall result in its continued approval being re-evaluated by the MGC on a continual basis;
- (D) The wireless deployment shall employ a secure gateway (e.g., firewall) to isolate the wireless environment from any other environment (e.g., the internal network). The secure gateway shall be configured in a manner that prevents any wireless network component from gaining access to the internal network without first being scrutinized. For each allowance defined within the secure gateway's access control list (i.e., policy) the following shall be documented:
 - (1) business requirement;
 - (2) source IP address, protocol, and port; and
 - (3) destination IP address, protocol, and port; and
- (E) All aspects of a wireless network, including all hardware and software utilized therein, shall be subject to testing by the MGC or an MGC licensed testing laboratory.

15.02 Written approval shall be obtained from the MGC prior to:

- (A) connecting or disconnecting any device or wireless network component from the wireless network infrastructure. This does not include supplicants or the replacement of previously approved wireless devices that have failed. The replacement devices shall be restored to MGC approved wireless configuration before connecting to the wireless system;
- (B) changing or modifying the configuration of any wireless network component; and
- (C) adding, removing, or modifying the configuration or access control lists used on the secure gateway.

§ 16 Compliance Assessments

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS

- 16.01 Every third calendar year, the Class A or Class B Licensee shall employ the services of an independent MIS security professional to assess the security of Critical IT Systems by performing a penetration test and a vulnerability and threat analysis assessment, and evaluating the licensee's compliance with MICS, Chapter S. An electronic copy of the report shall be submitted to the MGC within 60 days after the conclusion of the on-site testing.
- 16.02 Penetration testing shall include a vulnerability assessment of all Critical IT Systems. This shall include any location which houses Critical IT Systems.

§ 17 Player Tracking Systems

- 17.01 All player tracking system accounts shall be one of the following as previously defined and all rules for those respective accounts shall apply:
- (A) generic account;
 - (B) default account;
 - (C) service account; or
 - (D) user account.
- 17.02 Each employee of a Class B licensee with write capability to the player tracking system shall possess an MGC occupational license.
- 17.03 If an employee of a Class B Licensee who has access to the player tracking system is suspended subject to termination, terminated or transferred to another department, the individual's access shall be terminated within 72 hours of the change in status.
- 17.04 The player tracking system shall be logically secured through the use of passwords, biometrics, or other means approved in the Internal Control System.
- 17.05 Security parameters for passwords shall meet the following minimum requirements. These requirements apply to all accounts except for service accounts and generic accounts. The Internal Control System shall delineate security parameters for passwords, and to what extent the system is configurable in meeting the security parameter requirements.
- (A) Passwords shall expire at least every 90 days.
 - (B) Passwords shall be at least six characters comprised of two of the four character classes.
 - (C) Passwords shall be confidential.
 - (D) Accounts shall be automatically locked out after three failed login attempts. The system may release a locked out account after 30 minutes have elapsed.
- 17.06 The player tracking system shall maintain a history of changes made to patron accounts (points and comps) by Class B employees including name changes, point issuances, comp

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS

issuances, point redemptions, comp redemptions, and address changes. The history shall include either the last 12 months of changes or the last ten changes. The audit trail shall include the time and date of the changes and who processed the changes.

- 17.07 Changes to the player tracking system parameters, such as point structures, shall be authorized by a department independent of MIS. Changes shall be made by employees of the MIS department and documented. Documentation shall include:
- (A) time and date;
 - (B) nature of the change;
 - (C) employee that authorized the change; and
 - (D) MIS employee who made the change.
- 17.08 All player tracking system user accounts shall be logged out or the screen shall be locked after 15 minutes of inactivity.
- 17.09 Player tracking systems shall employ network-based time synchronization (e.g., network time protocol).
- 17.10 Personal identification numbers (PINs) shall be encrypted during electronic transmission and storage on player tracking systems. During storage, PINs shall be encrypted with at least a 128-bit key size.
- 17.11 Daily backup and recovery procedures shall be in place for player tracking systems.
- 17.12 The backup media shall be transferred within 96 hours to an off-site location separate from the location housing the servers and data being backed up for storage, unless otherwise approved by the MGC. The storage location shall be secured to prevent unauthorized access and shall provide protection to prevent the permanent loss of data in the event of a fire or other disaster.
- 17.13 The backup processes and procedures implemented for restoring data and application files shall be available upon request. The job position of the employee responsible for the backup shall be included in the Internal Control System.
- 17.14 If online access is provided for patrons to view their account balances or transaction histories from the player tracking system, physical or logical restrictions shall exist to provide independent operation from the player tracking system.
- 17.15 An encryption algorithm with a minimum of a 128-bit key size shall be utilized when transmitting or receiving player tracking system data to or from any source outside of the local intranet.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER S - MANAGEMENT INFORMATION SYSTEMS

- 17.16 Wireless player tracking systems shall comply with the rules set forth in the Wireless Network section of this chapter.

Note: Sections 313.800 through 313.850, RSMo, et seq., and Title 11, Division 45 of the Code of State Regulations establish standards to which Class B licensees must comply. Class B licensees should review these statutes and rules to ensure their ICS includes compliance with the requirements set forth. (Revised June 30, 2011). Revised October 30, 2013 (Sections 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 10.05, 11.01, and 12.04).