MISSOURI GAMING COMMISSION

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

CONTENTS

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

§ 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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

§ 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.

(A) Passwords shall expire at least every 90 days.

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

(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.

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.

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

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;
(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.

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

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:

(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.

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

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 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.

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

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, 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 in-bound 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.

§ 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).

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

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:

(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.

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

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;

(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

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

(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

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.

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

§ 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 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;

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).

(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.

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 June 30, 2014 (1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02).