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. (Adopted June 30, 2011). Revised, effective June 30, 2014 (revised 1.05, 4.02, 4.03, 4.05, 5.04, 7.02, 7.03, 10.05, 11.01, 12.04, and 13.02). Revised, effective September 30, 2022 (replaced sections 1, 4, and 15; removed 6.02; added 2.08-2.11, 5.07, 5.08, 14.03, and 14.05; revised 2.06, 3.01, 3.02, 3.04, 3.05, 5.04, 5.06, 6.03, 7.01, 7.02, 8.03-8.05, 9.01-9.03, 10.03, 10.05, 10.06, 12.01-12.04, 13.01, 14.01, 14.02. 14.04, 16.01, 16.02, 17.01, 17.05, 17.06, 17.08, and 17.13).

§ 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 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 "Bluetooth" is a wireless personal area network (WPAN) technology using a low power, short-range wireless communications protocol for the two-way interconnection of cellular phones, computers, and other electronic devices, including gaming devices. Bluetooth connections typically operate over distances of 10 meters or less and relies upon short-wavelength radio waves to transmit data bi-directionally over the air.

1.04 "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. ~!@#$%^&*()_+=-`[]{}\|;':",./<>?).

1.05 "Critical Information Technology (IT) System and equipment" includes all components of a network's hardware and software (e.g., slot accounting systems, bonusing systems, server supported game systems, cashless systems), application software, operating system, 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 "Generic accounts" are accounts shared by multiple users (using the same password) with access to Critical IT Systems and equipment.

1.07 "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.

1.08 "Local intranet" is a network which only includes the Class B Licensee's local facility.

1.09 "Management Information Systems (MIS) personnel" are employees that have been designated in the Internal Control System to perform the information technology functions for the operation of Critical IT Systems and equipment.

1.10 "Network hardware" includes all components that transmit gaming-related data on a network such as security appliances, switches, server(s), and Slot Machine Interface Boards (SMIBs) included in or critical to the operation of the Critical IT System.

1.11 "Remote access" refers to connectivity to the Class A or B Licensee's internal network from employees and vendors originating from sources outside the Class A or B Licensee's private network.

1.12 "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.

1.13 "Slot accounting system" is an on-line monitoring and control system that continuously monitors each approved gaming device via a defined communication protocol by either a dedicated line 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.

1.14 "System accounts" are service accounts on which automated system functions are dependent to execute and default accounts with predefined access levels created by the manufacturers at installation, which are necessary for configuration or proper operation.

1.15 "System administrator" is the individual(s) responsible for maintaining the stable operation of the critical IT system and equipment.

1.16 "Threat analysis" is the examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

1.17 "User accounts" are all accounts other than system accounts or generic accounts.

1.18 "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.

1.19 "Wi-Fi" is a wireless local area network (WLAN) technology using a wireless communication protocol for the interconnection of cellular phones, computers, and other electronic devices, including gaming devices within a particular area.

§ 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 accounts in the Critical IT System shall be one of the following:

(A) Generic account;
(B) System account; or
(C) 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.

2.08 The Class B Licensee shall provide the commission at least 30 days advance notice of any new installation and/or proposed programming changes to critical files of an existing Critical IT System through submission of an MGC System Upgrade Request (SUR). The SUR shall include the following information:

(A) Requestor full name;
(B) Email address;
(C) Description of the system upgrade;
(D) Project Coordinator name and phone number;

(E) Project start date and time;
(F) Project finish date and time;
(G) Reason if less than 30 days;
(H) Device type;
(I) Current ID number, if applicable;
(J) New ID number, if applicable;
(K) IP address, if applicable;
(L) Server name, if applicable; and
(M) Timeline of the project.

2.09 All Critical IT System user and system accounts shall be logged out or the screen shall be locked after 15 minutes of inactivity.

2.10 Should the Class B Licensee choose to configure a test environment off the gaming floor for training or testing purposes, the licensee shall submit detailed written correspondence to the MGC for approval. The Class B Licensee shall establish control procedures to ensure the following:

(A) Live production data (i.e., actual patron accounts) is not utilized for training or testing purposes;
(B) Adequate controls are in place for removal of all accounts and liability;
(C) Each individual participating in the test is assigned a uniquely identifiable account number which permits reconciliation;
(D) The training/testing environment has restricted access acceptable to the MGC;
(E) All ingress and egress to the testing area is documented and maintained until the training/testing environment is removed;
(F) A physically or logically segregated network is utilized between the test and production environments; and
(G) All controlled modules are approved for use in the State of Missouri, unless otherwise approved in writing by the MGC.

2.11 All files which are deemed to be critical for the proper operation of Critical IT Systems shall be designed to permit an on-demand, independent integrity check. The integrity check (i.e., authentication process) shall be accomplished utilizing a commission approved, external third-party verification tool.

§ 3 Physical Access and Maintenance Controls

3.01 Areas (e.g., rooms, cabinets, racks, etc.) housing any Critical IT System server shall be locked and access shall be restricted to MGC licensed MIS personnel with the use of a sensitive key or proximity card. All other individuals shall be escorted by a licensed MIS employee while accessing areas housing any Critical IT System server, with the exception of areas that solely house server supported game system servers which may be accessed by slot technicians, or above within the Slot department.

3.02 The Critical IT System 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 System server;
(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 or ports shall only be opened when access is required, and closed within 24 hours of use. The Class B Licensee shall keep a list of all network jacks or ports accessible to the public and their locations.

3.05 All communication closets (e.g., wiring closets) shall be locked when not occupied and shall have dedicated surveillance coverage. Only MGC licensed individuals shall have access to communication closets with the use of a sensitive key or proximity card. Non-licensed individuals shall be escorted by Security or licensed MIS personnel.

§ 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 System enforced security parameters for passwords shall meet the following minimum requirements. These requirements apply to all user accounts.

(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 All accounts that have administrative access over a Critical IT system (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.

4.05 Administrative access to the network, operating system, applications, and database security and system parameters shall be limited to licensed MIS personnel, both local and corporate, and supplier occupational licensees, unless otherwise approved in writing by MGC.

4.06 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.

4.07 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.

4.08 The Class A or Class B Licensee shall maintain and monitor Critical IT Systems and equipment to ensure proper operation and availability of the system.

4.09 All security incidents or malfunctions that affect the availability of the system shall be reported immediately in writing to the MGC agent on duty.

4.10 The Class B Licensee shall immediately notify the MGC in writing of any security breach to its Critical IT Systems and equipment.

4.11 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.

4.12 Critical IT System servers shall possess sufficient high availability features and employ redundancy techniques to prevent loss of data. The Class B Licensee shall submit written detailed topology layout, rapid recovery strategies and failover procedures via the MGC EGD Portal.

4.13 All Critical IT Systems shall employ network-based time synchronization (e.g., network time protocol).

4.14 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, position, or job group;
(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;
(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 who has Critical IT System access. 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.

5.07 Slot accounting system access cards (e.g., mechanic, slot host, global, etc.), except for cards used to capture meters, shall be uniquely numbered and assigned by an MGC licensed MIS employee or a Slot Technician Supervisor to occupational licensees employed by the Class B Licensee. Access cards shall only be assigned to employees who need the card to perform their job duties. An access card shall only be utilized by the employee to whom the card is assigned. The Class B Licensee shall maintain a list of each type of access card, its functions, and the job positions authorized to use that card. The MIS department or Slot department shall maintain documentation of all access card numbers and the employee assigned to each card. Additionally, any access card that could be used at other casinos (e.g., Global Global cards, etc.) shall be treated as a sensitive key.

5.08 User accounts assigned to a vendor shall only be operable for authorized use when a vendor requires access to Critical IT Systems and equipment.

§ 6 Generic Accounts

6.01 Generic accounts shall be restricted to read-only access.

6.02 Generic accounts shall be unique to each application. Generic accounts cannot exist across multiple applications.

6.03 The Class B Licensee shall identify in a submission to the MGC EGD Portal each generic account and its permissions that will be used to access Critical IT Systems.

6.04 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 System Accounts

7.01 System accounts shall be utilized in a manner to prevent unauthorized and inappropriate usage. System account passwords shall be changed prior to system implementation. The Internal Control System shall specify the method used to prevent unauthorized and inappropriate usage of all system accounts for all Critical IT Systems.

7.02 All system accounts with administrative access shall be disabled prior to system implementation unless they are necessary for proper operation of the system.

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 a period of no less than 365 days.

8.04 The Class B Licensee shall test data redundancy procedures to ensure data is retrievable from the backup media 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 Internal Control System shall identify the job position(s) responsible for the backup.

§ 9 Recordkeeping

9.01 Critical IT System documentation for all in-use versions of applications, databases, network hardware, and operating systems shall be provided upon request, 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 generic and system 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) The account status (i.e., enabled or disabled).

9.03 The current list of all enabled generic and system 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 Hardware or software (e.g., firewall, IPS, IDS, host-based intrusion system, etc.) 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 hardware or software, 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 MGC shall be executed no less than every 24 hours to monitor unauthorized modifications or corruption. Results of the integrity check shall be logged and maintained for at least 365 days. Should the system integrity check(s) fail, a notification shall be sent to the Class B Licensee designee, as noted in the Internal Control System, and the MGC shall be immediately notified in writing.

10.06 Unless otherwise recommended by the Critical IT System supplier, any physical or virtual asset containing a database used in conjunction with Critical IT System application software, and any physical or virtual asset containing Critical IT System files and directories must utilize anti-malware software. If signature-based anti-malware software is used, it shall be updated at least once every 7 days. If non-signature-based anti-malware software (e.g., heuristic, artificial intelligence, etc.) is used, it shall be updated according to the manufacturer's guidelines.

§ 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 to the Critical IT System(s) shall be granted/authorized through the use of Two-Factor Authentication (T-FA). The Internal Control System shall describe the two factors required.

12.02 Remote access to any Critical IT Systems and equipment shall be monitored by an Intrusion Detection System (IDS) or Intrusion Detection and Prevention System (IDPS).

12.03 For each Critical IT System that can be accessed remotely, the Internal Control System shall specifically address remote access methods and procedures and shall include, at a minimum:

(A) How user accounts and passwords are established to allow authorized, licensed individuals to access the system through remote access; and
(B) How the licensed MIS personnel enable remote access to the system when an authorized, licensed individual requires remote access to the system.

12.04 Vendor remote access shall require:

(A) Each remote access to a Critical IT System shall only be granted by a Class A or Class B licensed MIS employee and shall be documented on the Remote Access Log via the MGC EGD Portal which shall be submitted to the MGC EGD Department by the 10th day of each month;
(B) Whenever the authorized remote access connection is no longer required, 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 for remote access shall remain in an inoperable state on all operating systems, databases, network devices, and applications until needed. The account shall be returned to an inoperable state within 24 hours following the end of the vendor's remote access session; and
(D) The Critical IT System, the operating system, or a third party application 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. In addition the Class A or B licensee shall—

(1) Test the system or application used at least once every 90 days to ensure the monitoring system is functioning properly; and
(2) Retain the monitoring information for at least 365 days.

§ 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) The review and approval of requests for new programs or program changes by the MIS supervisory personnel. The review and approval shall be documented by the reviewing MIS supervisory personnel;
(B) Testing and certification by a licensed independent testing laboratory for software that has write privileges (e.g., changing data, modifying system configurations) into any Critical IT System;
(C) Approval from MGC prior to installation. In emergency situations, testing and certification may be subsequent to installation, if approved by MGC; and
(D) 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

14.01 Any purchased software that is a Critical IT System or has write privileges into any Critical IT System shall be submitted to an MGC licensed independent testing laboratory for testing and certification, and shall be approved by the MGC prior to use. If the purchased software utilizes an MGC approved gateway, it does not need to be submitted to an independent testing laboratory.

14.02 An SUR, available on the MGC EGD Portal, shall be submitted and approved prior to the installation of any new purchased software that has write privileges into any Critical IT System.

14.03 An SUR shall be submitted prior to upgrading any existing MGC approved purchased software with write privileges into a Critical IT System that does not utilize an MGC approved gateway.

14.04 Testing of new and modified purchased software 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.

14.05 Class B Licensees shall submit a list of purchased software programs with read or write privileges into a Critical IT System to the MGC EGD staff via the MGC EGD Portal. The list shall include:

(A) Software name;
(B) Software manufacturer;
(C) Software description;
(D) Software intended use;
(E) Version (if applicable);
(F) Indication the software is "Read-Only" or "Read and Write";
(G) Date implemented; and
(H) Gateway(s) utilized.

Any additions or modifications to the list shall be submitted to the MGC EGD staff within 96 hours after implementation or any upgrades.

§ 15 Wireless Networks

15.01 Wi-Fi used in conjunction with any Critical IT System and equipment:

(A) Submit in writing to the MGC for approval the proposed specific security standards, to include the version number(s), version date(s), and implementation date(s);
(B) Submit the MGC approved specific security standards including the version number(s), version date(s), and implementation date(s) via the MGC EGD Portal;
(C) Have an assessment completed prior to implementation to show compliance with Missouri statutes, regulations, MICS, and the Class B Licensee's chosen security standards for all wireless network aspects (e.g., hardware, software, authentication, repudiation, wireless client operation system hardening, etc.). The assessment shall be conducted by an independent MIS security professional. The report of this assessment shall be submitted to the MGC for evaluation. The wireless network shall not be used in a live environment until the MGC has approved the use of the wireless network based upon its evaluation of the report;

(D) Submit written notification of any physical or logical infrastructure changes to the wireless network in the live environment to the MGC for approval and update the MGC EGD Portal prior to implementation; and

(E) Document continued adherence to the adopted standards and provide the documentation to MGC upon request.

15.02 Wi-Fi used in conjunction with Critical IT Systems and equipment or player tracking systems must employ a secure gateway (e.g., firewall) to isolate the wireless environment from any other environment (e.g., the internal network).

15.03 Bluetooth used in conjunction with Critical IT Systems and equipment or player tracking systems shall receive MGC approval prior to deployment. To receive MGC approval the following requirements shall be met:

(A) Transmission power must be configured for proximity controls applicable to the use case (e.g., deployment at an EGD, table game, etc.) to ensure:

(1) A patron is carded out when walking away from a connected gaming device; and

(2) No interference or misreads occur upon a card in at a gaming device due to proximity to an adjacent wireless device; and

(B) The wireless network shall be configured for the maximum encryption level supported unless a degradation in performance or operational impact is proven, but no less than a minimum encryption of a 128-bit key size.

15.04 MIS personnel shall perform monthly vulnerability scans of all wireless networks used in conjunction with Critical IT Systems and equipment (e.g., Wi-Fi, Bluetooth). Vulnerability results shall be submitted via the MGC EGD Portal along with corresponding mitigation or remediation efforts. Vulnerabilities receiving a critical or high severity rating from the monthly vulnerability scan shall be remediated or the Class B Licensee shall establish mitigating controls within 90-days of the scan. If a critical vulnerability cannot be sufficiently addressed to provide the same security as a wired network, the MGC reserves the right to rescind approval of the use of the wireless network.

15.05 MIS personnel shall ensure that all patch management and firmware updates are performed on wireless networks within 90 days of the release date.

15.06 Gaming devices shall not be connected to the slot accounting system or a hybrid table game system via a wireless connection.

§ 16 Compliance Assessments

16.01 Every third calendar year, the Class A or Class B Licensee shall employ the services of an independent third party 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. Vulnerabilities receiving a critical or high severity rating from the penetration testing shall be remediated or the Class B Licensee shall establish mitigating controls within 90-days of the on-site testing. An electronic copy of the report shall be submitted to the MGC within 60 days after the conclusion of the on-site testing. The report shall include all findings and management's responses to the findings. The management responses shall include the specific corrective action to be taken, implementation date and the employee(s) responsible for implementation and subsequent follow-up. If the exception has already been addressed, the report shall include the corrective action taken and the date the corrective action occurred.

16.02 Penetration testing shall include a vulnerability assessment of all Critical IT Systems and equipment. This shall include:
(A) Any location which houses Critical IT Systems and equipment; and
(B) The testing of all aspects defined by MICS, Chapter S §15 for any wireless networks used in conjunction with Critical IT Systems and equipment.

§ 17 Player Tracking Systems

17.01 All accounts in the player tracking system shall be one of the following as previously defined and all rules for those respective accounts shall apply:
(A) Generic account;
(B) System account; or
(C) 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 user 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 eight characters comprised of three 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 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 shall be maintained. The history shall include either the last 12 months of changes or the last ten (10) 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 and system 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 positions of the employees 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.