STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INFORMATION TECHNOLOGY

Note 1: Unless otherwise specified, all Information Technology (IT) MICS apply to gaming and entertainment tax related applications, and the underlying databases and operating systems. Entertainment tax related applications include systems used to record admission ticket sales and point-of-sale systems used to record food, beverage, merchandise, admission and any other sales subject to live entertainment tax. If a person or entity other than the licensee offers entertainment subject to the entertainment tax on the licensee's premises, the entertainment tax related application being used shall be compliant with the IT MICS.

Note 2: The IT MICS do not apply when a person or entity other than the licensee operates a box office system for handling and recording live entertainment taxable admission sales (e.g., Ticket Master box office system). The IT MICS do apply when a licensee operates a box office system (for in-person sales or sales made through the Internet) for handling and recording live entertainment taxable admission sales.

Note 3: The types of gaming and entertainment tax related applications (including version numbers used) and the procedures and records used to comply with IT MICS #1 - #28, as applicable, must be addressed in detail in each applicable section, including the entertainment section, of the written system of internal control pursuant to Regulation 6.090. The Information Technology section of the written system of internal control pursuant to Regulation 6.090 includes the procedures and records used to comply with IT MICS #29 - #55, as applicable.

Note 4: Definitions. The following terminology and respective definitions are used in these MICS unless the context requires otherwise:

"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 usually provide detail on the type of backup performed, success or failure of the operation, and a list of errors.

"Critical IT systems and equipment" includes all components of systems hardware and software, application software, and database software that individually or in combination are necessary for the stable operation of gaming and entertainment systems. The term does not include user terminals.

"Default accounts" are user accounts with predefined access levels usually created by default at installation for operating systems, databases, and applications. These accounts tend to be used for training purposes.

"Generic user accounts" are user accounts that are shared by multiple users (using the same password) to gain access to gaming and entertainment systems and applications.

"Group membership" (group profile) is a method of organizing user accounts into a single unit (by job position) 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.

"IT personnel" are employees who are independent of the gaming and entertainment department; and have been designated to perform the information technology function for the operation of critical IT systems and equipment.

"Physical and logical segregation of the development and testing from the production environment" is separating the development and testing of new software in an environment that is isolated from the regular production (live) network. The development environment is located on a separate server and developers are precluded from having access to the production environment.

"Secured repository" is a secured environment that is used to store software source code once it has been approved for introduction into the production (live) environment. The repository is secured such that developers cannot modify code once it has been stored. In this way, the repository provides a history of a given software system ordered by version.

INFORMATION TECHNOLOGY

“Service accounts” are accounts on which automated system functions are dependent to execute. These accounts defined at the operating system level provide a certain level of access necessary for normal operation of applications and/or automated batch processes.

“System administrator” is the individual(s) responsible for maintaining the stable operation of the IT environment (including software and hardware infrastructure and application software).

“Vendor supported system” is one type of critical IT systems and equipment; however, this type of system is supported solely by the manufacturer of such system.

Physical Access and Maintenance Controls

1. The critical IT systems and equipment for each gaming application (e.g., keno, race and sports, slots, cashless wagering systems, etc.) and each application for entertainment are maintained in a secured area. The area housing the critical IT systems and equipment for each gaming and entertainment application and other critical IT systems and equipment are equipped with the following:

   a. Redundant power sources to reduce the risk of data loss in case of interruption of power.

   Note: MICS #1(a) does not apply to components in the slot gaming device cabinet.

   b. An adequate security mechanism, such as traditional key locks, biometrics, combination door lock, or electronic key card system to prevent unauthorized physical access to areas housing critical IT systems and equipment for gaming and entertainment applications.

2. Access to areas housing critical IT systems and equipment for gaming and entertainment applications, excluding vendor supported systems, is restricted to authorized IT personnel. Gaming and entertainment department personnel, including the manufacturers of the gaming and entertainment computer equipment, are only allowed access to the areas housing critical IT systems and equipment for gaming and entertainment applications, excluding vendor supported systems, when authorized by IT personnel and with periodic monitoring by IT personnel during each access. A record of each access by non-IT personnel is maintained with the name of the visitor(s), time and date of arrival, time and date of departure, reason for visit and the name of IT personnel authorizing such access.

3. Access to an area housing a vendor supported system for gaming and entertainment applications is restricted to authorized IT personnel, or by system manufacturer’s personnel when authorized by management and with periodic monitoring during each access by IT personnel or personnel independent of the department using such application. A record of such access by the system manufacturer’s personnel is maintained with the name of the visitor(s), time and date of arrival, time and date of departure, and reason for visit.

4. The administration of the electronic security systems, if used to secure areas housing gaming and entertainment critical IT systems and equipment, is performed by personnel independent of a gaming or entertainment department.

System Parameters

5. The computer systems, including application software, are logically secured through the use of passwords, biometrics, or other means approved by the Board.

6. Security parameters for passwords, if configurable, shall meet the following minimum requirements:

   a. Passwords are changed at least once every 90 days.

INFORMATION TECHNOLOGY

b. Passwords are at least 8 characters in length and contain a combination of at least two of the following criteria: upper case letters, lower case letters, numeric and/or special characters.

c. Passwords may not be re-used for a period of 18 months; or passwords may not be re-used within the last ten password changes.

d. User accounts are automatically locked out after 3 failed login attempts.

Note 1: The written system of internal control is to delineate whether the system is configurable for security parameters for passwords, and to what extent the system is configurable in meeting the security parameter requirements.

Note 2: MICS #6 does not apply to service accounts and generic user accounts.

Note 3: For MICS #6(d), the system may release a locked out account after 30 minutes has elapsed.

7. A system event log or series of reports/logs for operating systems (including the network layer) and gaming and entertainment applications, if capable of being generated by the system, is configured to track the following events:

a. Failed login attempts.

b. Changes to live data files occurring outside of normal program and operating system execution, if configurable.

c. Changes to operating system, database, network, and application policies and parameters, if configurable.

d. Audit trail of information changed by administrator accounts, if configurable.

e. Changes to date/time on master time server, if configurable.

Note: For MICS #7 the written system of internal control is to delineate whether the system is configurable, and to what extent the system is configurable, in tracking specified events.

8. Daily system event logs are reviewed at least once a week (for each day of the entire previous week) by IT personnel, other than the system administrator, for events listed in MICS #7. The system event logs are maintained for a minimum of seven days, consisting of the period previously reviewed. Evidence of this review (e.g., log, checklist, notation on reports) is maintained for a minimum of 90 days and includes the date, time, name of individual performing the review, the exceptions noted, and any follow-up of the noted exception.

Note: For MICS #8 an automated tool that polls the event logs for all gaming and entertainment related servers, and provides the system administrators notification of the above may be used. Maintaining the notification for 90 days may serve as evidence of the review.

9. Exception reports, if capable of being produced by the system, (e.g., changes to system parameters, corrections, overrides, voids, etc.) for each gaming application and entertainment tax related application are maintained and include at a minimum:

a. Date and time of alteration;

b. Identification of user that performed alteration;

c. Data or parameter altered;

d. Data or parameter value prior to alteration; and

e. Data or parameter value after alteration.

Note: The written system of internal control is to indicate the system's capability of producing an exception report and to what extent this report provides specified information.

User Accounts

10. Management personnel, or persons independent of the department being controlled, establish, or review and approve, user accounts for new employees. Provisioning for user accounts consist of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties.

11. Provisioning of user accounts for employees who transfer to a new department are performed, or reviewed and approved, by management personnel, or persons independent of the department being controlled. Any previously assigned application function access for the employee's user account is changed to inactive (disabled) prior to the employee accessing their new user account for their role or position in a new department.

12. User access listings include, if the system is capable of providing such information, at a minimum:

    a. Employee name and title or position.

    b. User login name.

    c. Full list and description of application functions that each group/user account may execute.

    Note: This list for MICS #12(c) may be available in a separate report if the menu functions are easily referenced between the user access listing report and the menu function report.

    d. Date and time account created.

    e. Date and time of last login.

    f. Date of last password change.

    g. Date and time account disabled/deactivated.

    h. Group membership of user account, if applicable.

    Note: The written system of internal control is to indicate the system's capability of producing a user access listing and to what extent the system's listing provides specified information.

13. When multiple user accounts for one employee per application are used, only one user account may be active (enabled) at a time if the concurrent use of the multiple accounts by the employee could create a segregation of duties deficiency resulting in noncompliance with one or more MICS. Additionally, the user account has a unique prefix/suffix to easily identify the users with multiple user accounts within one application.

14. The system administrator is notified within a reasonable period of time, established by management, when an employee is known to be no longer employed (e.g., voluntary or involuntary termination of employment). Upon notification the system administrator changes the status of the employee's user account from active to inactive (disabled) status. The written system of internal control pursuant to Regulation 6.090 delineates the process and reasonable time period in notifying the system administrator for updating the terminated employee's user account and the procedures established in preventing the employee from having unauthorized access to a user terminal.

Note: The reasonable period of time in notifying the system administrator to change the status of the terminated employee's user account assumes that it is relatively unlikely the employee will have unauthorized access to a user terminal during that time period.

15. The system administrator is notified as soon as possible when an employee who has a user account with remote access capability is known to be no longer employed (e.g., voluntary or involuntary termination of employment). Upon notification the system administrator changes the status of an employee’s user account with remote access capability from active to inactive (disabled) status. The written system of internal control pursuant to Regulation 6.090 delineates the process in notifying the system administrator as soon as possible for immediately updating the terminated employee's user account with remote access capability and the procedures established in preventing the employee from having unauthorized remote access.

Note: During the period of time when the employee is no longer employed and until the user account has been disabled, it is assumed that it is relatively unlikely the employee will have unauthorized remote access to the system during that time period.

16. User access listings for gaming applications at the application layer are reviewed quarterly by personnel independent of the authorization and user provisioning processes. The review consists of examining a sample of at least 10% (with a maximum of 25) of the users included in the listing. The reviewer maintains adequate evidence to support the review process, which includes the identified accounts reviewed, documentation of the results of the review, and e-mails or signatures and dates indicating when the user access listing was reviewed. For each of the randomly selected users, determine whether:

a. The assigned system functions are being used as authorized (i.e., system functions are appropriate for user’s job position);

b. The assigned functions provide an adequate segregation of duties;

c. Terminated employees user accounts have been changed to inactive (disabled) status;

d. Passwords have been changed within the last 90 days; and

Note: The review for password changes within 90 days applies regardless of whether the system parameter has been configured to have the password changed at least once every 90 days [as required by MICS #6(a)].

e. There are no inappropriate assigned functions for group membership, if applicable.

Note 1: The required review of user access listings does not apply to user access listings for pari-mutuel systems and for any entertainment tax related applications.

Note 2: The review applies to user access listings for computerized gaming systems with the following capabilities:

- Generates reports identifying gaming revenues;
- Generates detailed records of all markers, IOU’s, returned checks, hold checks, or other similar credit instruments;
- Generates statistical gaming records required by the MICS; or
- Generates any other records required either by the MICS or by the licensee’s system of internal control.

Note 3: MICS #16(e) applies to a review of the assigned functions for the selected user account with group membership.

Generic User Accounts

17. Generic user accounts at the operating system level, if used, are configured such that the user is automatically brought to the application logon screen immediately upon logging into the operating system. The generic user accounts must also be configured such that the user is logged out of the operating system automatically upon exiting the application.

18. Generic user accounts at the application level, are prohibited unless user access is restricted to inquiry only functions or is specifically allowed in other sections of the MICS.

Service & Default Accounts

19. Service accounts, if used, are utilized in a manner to prevent unauthorized and inappropriate usage to gain logical access to an application and the underlying databases and operating system. The employee responsible for the documentation indicating the method used to prevent unauthorized and inappropriate usage of these service accounts (available upon request by authorized internal and external auditors and by Board personnel) is delineated in the written system of internal control pursuant to Regulation 6.090.

    Note: Suggested methods include: (1) Service accounts are configured such that the account cannot be used to directly log in to the console of a server or workstation; (2) Service account passwords are to be changed at least once every 90 days, and immediately upon termination of system administrators.

20. User accounts created by default (default accounts) upon installation of any operating system, database or application are configured to minimize the possibility that these accounts may be utilized to gain unauthorized access to system resources and data. The employee responsible for the documentation indicating the procedures implemented to restrict access through the use of default accounts (available upon request by authorized internal and external auditors and by Board personnel) is delineated in the written system of internal control pursuant to Regulation 6.090.

21. Any other default accounts that are not administrator, service, or guest accounts should be disabled unless they are necessary for proper operation of the system. If these accounts must remain enabled, the passwords are changed at least once every 90 days.

Administrative Access

Note: Administrative access means access that would allow a user to:

- Add, change, or delete user accounts and associated user provisioning
- Modify operating system, database, and application security and policy parameters
- Add, change, or delete system exception logging information
- Add, change, or delete permissions to data files and folders

22. Access to administer the network, operating system, applications, and database security and system parameters is limited to supervisory and/or management employees of the IT department or IT employees under the supervision of supervisory and/or management employees of the IT department. If there is no IT department, supervisory or management personnel independent of the department using such system and/or application may perform the administrative procedures.

23. Systems being administered are enabled to log usage of all administrative accounts, if provided by the system. Such logs are maintained for 30 days and include time, date, login account name, description of event, the value before the change, and the value after the change.

24. An individual independent of the slot department daily reviews the requirements of a system based game and a system supported game ensuring the proper use of split or dual passwords by system administrators [requirements listed at Regulation 14, Technical Standards 1.084(4) and 1.086(4)].

Note: MICS #24 requires a review to confirm that the system requires the use of split or dual passwords and that split or dual passwords have been used.

Backups

25. Daily backup and recovery procedures are in place and, if applicable, include:

    a. Application data.

    Note: This standard only applies if data files have been updated.

    b. Application executable files (unless such files can be reinstalled).

    c. Database contents and transaction logs.

26. Upon completion of the backup process, the backup media is immediately transferred to a location separate from the location housing the servers and data being backed up (for temporary and permanent storage). The storage location is secured to prevent unauthorized access and provides adequate protection to prevent the permanent loss of any data.

    Note 1: Backup data files and programs can be maintained in a secured manner in another building on the premises that is physically separated from the building where the system's hardware and software are located. They may also be stored in the same building as the hardware/software as long as they are secured in a fireproof safe or some other manner that will ensure the safety of the files and programs in the event of a fire or other disaster.

    Note 2: MICS #26 does not apply to backup data files for computerized keno and bingo systems except for inter-casino linked keno games or keno games that accept multi-race keno wagers that will not be completed by the end of the next gaming day.

27. Backup system logs, if provided by the system, are reviewed daily by IT personnel or individuals authorized by IT personnel to ensure that backup jobs execute correctly and on schedule. The backup system logs are maintained for the most recent 30 days.

28. The employee responsible for the documentation indicating the procedures implemented for the backup processes and for restoring data and application files (available upon request by authorized internal and external auditors and by Board personnel) is delineated in the written system of internal control pursuant to Regulation 6.090.

    Note: While not mandatory, licensees are encouraged to test recovery procedures at least annually.

Recordkeeping

29. System documentation for all in-use versions of applications, databases, network hardware, and operating systems is maintained, including descriptions of both hardware and software (including version numbers), operator manuals, etc.

30. System administrators maintain a current list of all enabled generic, system, and default accounts. The documentation includes, at a minimum, the following:

    a. Name of system (i.e., the application, operating system, or database).

    b. The user account login name.

    c. A description of the account's purpose.

d. A record (or reference to a record) of the authorization for the account to remain enabled.

31. The current list is reviewed by IT management in addition to the system administrator at least once every six months to identify any unauthorized or outdated accounts.

32. User access listings (requirements listed at MICS #12) for all gaming systems are to 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 preclude alteration). If available, the list of users and user access for any given system is in electronic format that can be analyzed by analytical tools (i.e., spreadsheet or database) that may be employed by Board agents.

Note: User access listings do not need to be retained for pari-mutuel systems and for any entertainment tax related applications.

33. The IT department maintains current documentation with respect to the network topology (e.g., flowchart/diagram), deployment of servers housing applications and databases, and inventory of software and hardware deployed (available upon request by authorized internal and external auditors and by Board personnel). The employee responsible for maintaining the current documentation on the network topology is delineated in the written system of internal control pursuant to Regulation 6.090.

Electronic Storage of Documentation

34. Documents may be scanned or directly stored to unalterable media (secured to preclude alteration) with the following conditions:

a. The storage media must contain the exact duplicate of the original document.

b. All documents stored must be maintained with a detailed index containing the casino department and date in accordance with Regulation 6.040(1). This index must be available upon Board request.

c. Upon request by Board agents, hardware (terminal, printer, etc.) must be provided in order to perform audit procedures.

d. Controls must exist to ensure the accurate reproduction of records, up to and including the printing of stored documents used for audit purposes.

e. At least quarterly, accounting/audit personnel review a sample of the documents on the storage media to ensure the clarity and completeness of the stored documents.

35. If source documents and summary reports are stored on alterable storage media, the media may not be relied upon for the performance of any audit procedures, and the original documents and summary reports must be retained.

Creation of Wagering Instruments Database

Note: MICS #36 - #39 apply when creating a database of wagering instruments that will be accepted by a cashless wagering system.

36. An individual independent of the gaming area performs the database creation and, if applicable, the creation of wagering instruments to be accepted in the cashless wagering system.

37. A record is maintained detailing the database creation and the wagering instruments to be accepted by the cashless wagering system, including evidence of user acceptance, date in service, and personnel involved.

38. Monthly, the wagering instrument database is reviewed and tested by personnel of the applicable gaming area and accounting/audit personnel for any improprieties.

39. The procedures used and subsequent results relating to the wagering instruments database review and test are documented and maintained.

Network Security

40. If guest networks are offered (such as, networks that provide internet access for patrons, hotel guests, or vendors), adequate logical segregation is provided of the guest network from the network used to serve access to gaming and entertainment tax related applications and devices. Traffic on guest networks is non-routable to the network serving gaming and entertainment tax related applications and devices.

41. Production networks serving gaming/entertainment systems are secured from outside traffic (e.g., firewall and routers) such that systems are configured to detect and report security related events. The employee responsible for the documentation indicating the procedures for detecting and reporting security related events (available upon request by authorized internal and external auditors and by Board personnel) is delineated in the written system of internal control pursuant to Regulation 6.090.

    Note: A suggested method in complying with MICS #41 is to configure the system to log unauthorized logins, failed login attempts, and other security related events; and block all unused ports and any in-bound connections originating from outside the network.

42. Network shared drives containing application files and data for all gaming and entertainment tax related applications are secured such that only authorized personnel may gain access.

43. Server consoles, and unattended user terminals in gaming areas, are configured to automatically secure themselves after a configurable period of inactivity elapses, the amount of time to be determined by management. The time period of inactivity is documented in the written system of internal control pursuant to Regulation 6.090. Users are to supply proper login credentials to regain access to the terminal or console.

44. Login accounts and passwords required to administer network equipment are secured such that only authorized IT personnel may gain access to these devices. The passwords for these accounts meet the security parameters of IT MICS #6, and are immediately disabled when IT personnel are terminated.

Changes to Production Environment

45. The employee responsible for the documentation indicating the process for managing changes to the production environment (available upon request by authorized internal and external auditors and by Board personnel) is delineated in the written system of internal control pursuant to Regulation 6.090. This process includes at a minimum:

    a. Proposed changes to the production environment are evaluated sufficiently by management personnel prior to implementation;

    b. Proposed changes are properly and sufficiently tested prior to implementation into the production environment;

    c. A strategy of reverting back to the last implementation is used (rollback plan) if the install is unsuccessful and the rollback plan is tested prior to implementation to the production environment; and

    d. Sufficient documentation is maintained evidencing management approvals, testing procedures and results, rollback plans, and any issues/resolutions encountered during implementation.

Note: The above process includes ALL changes to the production environment (operating system, network, databases, and applications) that relate to critical IT systems, and gaming and entertainment applications.

Remote Access

46. For each computerized gaming or entertainment tax related application that can be accessed remotely for purposes of obtaining vendor support, the written system of internal control pursuant to Regulation 6.090 must specifically address remote access procedures including, at a minimum:

    a. Type of gaming or entertainment tax related application, vendor’s name and business address (business address only for cashless wagering systems) and version number, if applicable.

    b. For cashless wagering systems only, the approved secured connection used so that the system can only be accessed from the vendor’s place of business.

    c. For a system based game and a system supported game, the method and procedures used in meeting the requirements of Regulation 14, Technical Standard 1.066.

    d. The method and procedures used in establishing and using passwords to allow authorized vendor personnel to access the system through remote access.

    e. 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.

    f. The personnel involved and procedures performed to ensure the method of establishing remote access connection is disabled when the remote access is not in use.

    g. Any additional requirements relating to remote access published by the Board.

47. In the event of remote access, prepare a complete record of the access to include: name or identifier of the licensee’s employee authorizing access, name or identifier of manufacturer’s employee accessing system, name of user account that vendor used, name of vendor, name of system(s) accessed by the vendor, description of work performed, date, time, and duration of access. The description of work performed must be adequately detailed to include the old and new version numbers of any software that was modified, and details regarding any other changes made to the system.

48. User accounts used by vendors must remain disabled on all operating systems, databases, network devices, and applications until needed by such vendor. Subsequent to an authorized use by a vendor, the account is returned to a disabled state.

49. Remote access for all vendors is enabled only when approved by authorized IT personnel.

50. If remote access to the production network (live network) is available, and allows access to gaming and entertainment tax related applications, such access is logged automatically by the device or software where it is established.

Information Technology Department

Note: If a separate IT department is maintained or if there are in-house developed systems, MICS #51 through #55 are applicable.

51. The IT department is independent of all gaming departments (e.g., cage, pit, count rooms, etc.) and operational departments subject to live entertainment tax.

52. IT personnel are precluded access to wagering instruments and gaming related forms (e.g., slot jackpot forms, table games fill/credit forms, etc.).

In-House Software Development

53. If source code for gaming and entertainment tax related software is developed or modified internally, a process is adopted to manage the development. The employee responsible for the documentation indicating the process in managing the development or modification of source code (available upon request by authorized internal and external auditors and by Board personnel) is delineated in the written system of internal control pursuant to Regulation 6.090. The process must address, at a minimum:

    a. Requests for new programs or program changes are reviewed by the IT supervisory personnel. Approvals to begin work on the program are documented.

    b. A written plan of implementation for new and modified programs is maintained and includes, at a minimum, the date the program is to be placed into service, the nature of the change (if applicable), a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who is to perform all such procedures.

    c. Sufficiently documenting software development and testing procedures.

    d. Documentation of approvals, development, testing, results of testing, and implementation into production. Documentation includes a record of the final program or program changes, including evidence of user acceptance, date in service, programmer, and reason for changes, is documented and maintained.

    e. Physical and logical segregation of the development and testing from the production environments.

    f. Adequate segregation of duties (i.e., those who develop/test code do not have access to introduce new or modified code into the production environment).

    Note: For MICS #53(e) and (f) a system administrator is precluded from developing/testing code which will be introduced into the production environment.

    g. Secured repositories for maintaining code history.

    h. End-user documentation (guides and manuals).

54. A copy of the associated equipment reporting form submitted to the Board pursuant to Regulation 14 for each new program or program change, and a record that such software was approved for use, is maintained.

Purchased Software Programs

55. New programs and program changes for purchased systems are documented as follows:

    a. Documentation is maintained and includes, at a minimum, the date the program was placed into service, the nature of the change (if applicable), a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who performed all such procedures.

    b. A copy of the associated equipment reporting form submitted to the Board pursuant to Regulation 14 for each new program or program change, and a record that such software was approved for use, is maintained.

c. Testing of new and modified programs is performed (by the licensee or the system manufacturer) and documented prior to full implementation.