

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

Note 1: Pursuant to Regulation 5A.140, interactive gaming is limited to the game of poker. Furthermore, the Card Games MICS do not apply to interactive gaming.

Note 2: Unless otherwise specified, all Information Technology for Interactive Gaming MICS apply to an interactive gaming application, the underlying database, operating system, and network layer.

Note 3: Interactive gaming operator must specify in their system of internal control pursuant to Regulation 6.090 which functions (if any) are performed by a third-party provider. Operators remain responsible for proper design and operational effectiveness of all required minimum internal control standards, regardless of who is performing the function.

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

Information Technology for Interactive Gaming

“Authorized player system” is the hardware and software used to execute authorized player software for the purpose of conducting interactive gaming and related activities. (“Authorized player software” is defined in the Technical Standards)

“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 interactive gaming system. The term does not include authorized player systems and other operator 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.

“Game session” is a semi-permanent interactive exchange of information between an authorized player system and the interactive gaming system that consists of all activities and communications performed by an authorized player and the interactive gaming system for the duration of the game. For the purpose of poker, a “game” is defined as a hand of poker that starts with an ante or blind wager being placed and ends with a determination of the winner(s) of the hand and subsequent payment to the winner(s).

“Generic user accounts” are user accounts that are shared by multiple users (using the same password) to gain access to any component of an interactive gaming system: application, database, or operating system.

“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 operation of interactive gaming; and who have been designated to perform the information technology function for the operation of critical IT systems and equipment.

“Player session” is a semi-permanent interactive exchange of information between an authorized player system and the interactive gaming system that consists of all activities and communications performed by an authorized player and the interactive gaming system between the time the authorized player logs into the interactive gaming system to the time the authorized player logs out or is logged out of the interactive gaming system.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

“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.

“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).

Physical Access and Maintenance Controls

1. The written system of internal control pursuant to Regulation 6.090 delineates the physical location of each component of the interactive gaming system, including the location of staff (operator, service provider, datacenter operator if the datacenter is maintained by an independent party).
2. The written system of internal control pursuant to Regulation 6.090 delineates the responsibilities of staff (operator, service provider, datacenter operator if the datacenter is maintained by an independent party) for operation, service and maintenance of interactive gaming system and/or its components.
3. The critical IT systems and equipment for the interactive gaming system are maintained in a secured area. The areas must be equipped with controls to provide physical protection against damage from flood, fire, earthquake and other forms of natural or manmade disasters and include at a minimum:
 - a. Redundant power sources to reduce the risk of data loss in case of interruption of power.
 - b. Adequate climate control and fire suppression equipment.
 - c. Other measures to ensure physical protection of hardware and software.
 - d. Adequate security mechanisms, 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 the interactive gaming system.

Note: The written system of internal control pursuant to Regulation 6.090 is to delineate the methods, processes and practices meeting the requirements of MICS #3 (a through d).

4. Access to areas housing critical IT systems and equipment for the interactive gaming system is restricted to authorized IT personnel. Non-IT personnel, including the manufacturers of the interactive gaming system’s computer equipment, are allowed access to the areas housing critical IT systems and equipment for the interactive gaming system only when authorized and accompanied by IT personnel and with continuous 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.
5. The administration of the physical access security mechanism used to secure areas housing the interactive gaming critical IT system and equipment, is performed by authorized IT personnel.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

Network Security

6. Production networks serving gaming/entertainment systems are secured from outside traffic (e.g., firewall and routers) and 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 is delineated in the written system of internal control pursuant to Regulation 6.090.

Note: A suggested method for complying with MICS #6 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.

7. Network shared drives containing application files and data for interactive gaming system are secured such that only authorized personnel may gain access.
8. Login accounts and passwords required to administer network and other 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 MICS #21, and accounts are immediately disabled when IT personnel are terminated.

Remote Access

9. Remote access to the interactive gaming system components (production servers, operating system, network infrastructure, application, database and other components) should be limited to appropriate IT department personnel employed by the operator of the interactive gaming system.
10. Remote access by vendor personnel to any component of the interactive gaming system is allowed for purposes of support or updates and is enabled only when approved by authorized IT personnel employed by the interactive gaming system operator. If the remote access to a database is performed by unlicensed vendor personnel, the remote access must be continuously monitored by IT personnel employed by the operator of the interactive gaming system.
11. When the interactive gaming system (or its components) can be accessed remotely for purposes of vendor support, the written system of internal control pursuant to Regulation 6.090 must specifically address remote access procedures including, at a minimum:
 - a. The component(s) of an interactive gaming system requiring vendor support and vendor name(s).
 - b. The method and procedures used to gain access remotely, including the use passwords and other logical controls.
 - c. The procedures to be used by IT personnel employed by the operator of the interactive gaming system to further control and monitor access, and to ensure that vendors have only the access needed to perform authorized support and update functions.
12. In the event of remote access by a vendor, a complete record of the access must be created and include at a minimum:
 - a. Name or identifier of the licensee's employee authorizing access;
 - b. Name of vendor
 - c. Name or identifier of vendor employee accessing system;
 - d. Name of user account through which the vendor employee accessed the system;

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- e. System component(s) accessed by the vendor;
 - f. Adequate and detailed description of work performed; and
 - g. Date, time, and duration of access.
13. Vendor accounts must be restricted through logical security controls to have the ability to access only the application(s) and/or database(s) that are necessary for the purposes of support or providing updates/upgrades.
14. The interactive gaming operator must employ security methods in addition to passwords to verify the identity of vendor personnel prior to the authorizing any remote access for that vendor.
15. 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.
16. Remote access may be allowed for non-IT personnel (management personnel or other authorized employees of the interactive gaming operator), but must be limited to only the application functions necessary to perform their job duties. Non-IT personnel must be precluded from directly accessing any databases or operating systems of any of the interactive gaming system and other production environment servers. Additional security methods must be employed beyond passwords for user accounts to ensure that interactive gaming system application and data integrity are maintained and secure.
17. Remote access to the interactive gaming system components is logged.
18. Remote access logs and records must be reviewed by accounting/audit personnel at least once each quarter on a sample basis to ensure that:
- a. Vendor accounts are inactive when not in use;
 - b. Terminated employees have not logged in;
 - c. Each remote access session has been appropriately recorded for vendors; and
 - d. Employees with remote access are authorized to have such access.
19. Evidence of the review of logs and records of remote access is maintained.

System Parameters

20. The interactive gaming system, including application software, is logically secured through the use of passwords, biometrics, or other means approved by the Board.
21. Security parameters for passwords shall meet the following minimum requirements:
- a. Passwords are changed at least once every 90 days.
 - 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.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

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

Note 1: The written system of internal control pursuant to Regulation 6.090 is to delineate the methods used to comply with MICS #21(b) and (c).

Note 2: MICS #21 does not apply to service accounts and generic user accounts.

Note 3: For MICS #21(d), the system may release a locked out account after 30 minutes has elapsed.

22. A system event log or series of reports/logs for operating systems (including the network layer) and applications is configured to track at least the following events:
- a. Failed login attempts.
 - b. Changes to live data files occurring outside of normal program and operating system execution.
 - c. Changes to operating system, database, network, and application policies and parameters.
 - d. Audit trail of information changed by administrator accounts.
 - e. Changes to date/time on master time server.
 - f. Significant periods of unavailability of the interactive gaming system or any critical component of the interactive gaming system; and
 - g. Other significant events (the written system of internal control pursuant to Regulation 6.090 is to delineate what other events are to be logged).
23. The interactive gaming system performs self-monitoring of critical components (e.g. central hosts, network devices, firewalls, links to third parties, etc.). A critical component which fails self-monitoring tests must be taken out of service immediately and not returned to service until the fault has been rectified. A log of this event is generated.
24. 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 #22 and #23. The system event logs are maintained for a minimum of seven days following the review.
25. The review described in MICS #24 must be documented, and evidence of this review must be maintained for 18 months following the completion of the review. The evidence is to include:
- a. Date and time of review;
 - b. Name and title of person performing the review;
 - c. Any exceptions noted;
 - d. Follow-up and resolution of exceptions.

Note: Compliance with MICS #24 and #25 may involve the use of an automated tool that “flags” the events for the interactive gaming system and provides the person assigned to complete the review with notification. A record of the notification should include the date and time of the notification.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

26. Exception reports for the interactive gaming system are configured to track the following events occurring outside the normal course of system operation that require employee intervention including, but not limited to:
- a. Adjustments to an authorized player's interactive gaming account balance;
 - b. Changes made to information recorded in an authorized player's interactive gaming account;
 - c. Changes made to an authorized player's self-exclusion limits;
 - d. Changes made to game parameters (e.g., game rules, payout schedules, rake percentage);
 - e. Changes made to payout parameters;
 - f. Voids, overrides, corrections;
 - g. Mandatory deactivation of an authorized player; and
 - h. Any other activity requiring employee intervention and occurring outside of the normal scope of system operation.
27. Exception reports produced for the interactive gaming system for the events listed in MICS # 26 include at a minimum:
- a. Date and time of the exception event;
 - b. Unique transaction identifier;
 - c. Identification of user who performed and/or authorized alteration;
 - d. Data or parameter altered;
 - e. Data or parameter value prior to alteration; and
 - f. Data or parameter value after alteration.

Structure of Information Technology Department

28. IT personnel are precluded from having access to any physical forms/documentation associated with patrons' accounts and interactive gaming (e.g., deposit/withdrawal slips, checks, etc.).

Note: Administrative access means access that would allow a user (i.e., system administrator) to:

- Add, change, or delete user accounts and associated user provisioning;
- Modify operating system, network, database, and application layers' security and policy parameters;
- Add, change, or delete system exception logging information; or
- Add, change, or delete permissions to data files, folders, libraries, tables, or databases

29. Access to administer the network, operating system, applications, and database security and system parameters is limited to:
- a. Supervisory and/or management employees of the IT department; or
 - b. IT employees under the supervision of supervisory and/or management employees of the IT department; or

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- c. Employees of operator/service provider of interactive gaming under the supervision of supervisory and/or management employees of the IT department.

Note: The written system of internal control pursuant to Regulation 6.090 is to delineate the assignment of administrative access and function for various components of the interactive gaming system.

- 30. Interactive gaming system and its components being administered are enabled to log usage of all administrative accounts. Such logs are to be maintained and include time, date, login account name, description of event, the value before the change, and the value after the change.
- 31. Administrative access at the operating system level for all servers that support or are part of the interactive gaming system must be reviewed quarterly. Reviews are performed by personnel independent of the IT department and include a complete review of all user accounts with administrative access. The reviewer performs the following:
 - a. Review all administrative groups and groups with elevated privileges to ensure membership is appropriate.
 - b. Review all service, generic, and default accounts to ensure that they are not enabled for remote access.
 - c. Review the last login date and time for all administrative accounts to determine whether any "stale" accounts exist (e.g., users on extended leave or terminated IT employees remain active in the system).
 - d. Review administrative accounts to ensure that passwords have been changed at least once every 90 days.
 - e. Examine user list to determine whether IT personnel utilize normal user accounts for regular use and administrator accounts for administrative functions.
 - f. Examine generic and service accounts to determine the method used to secure them from unauthorized usage is a properly designed control process and operating effectively.
 - g. Documentation of the results of the review is retained for a period of 18 months and includes the date, time, and name and title of the person performing the review.

User Accounts

- 32. A system administrator is to establish user accounts for new employees and employees who transfer to a new department. Provisioning for user accounts consists of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties. The transferred employees must have access appropriate for the new position only when the access for the previous position has been removed or disabled.
- 33. The access provisioning process must be documented; documentation must evidence authorization by the appropriate management personnel, original user access and each subsequent change to user account; documentation must be maintained and made available upon request.
- 34. A "User Access Listing" report must be produced by the interactive gaming system and contain at a minimum:
 - a. Employee name and title or position.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- b. User login name.
- c. Full list and description of application functions that each group/user account may execute.
- 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.

35. When multiple user accounts are used for one employee within a single application, 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. Additionally, the user account has a unique prefix/suffix to easily identify the users with multiple user accounts within one application.

36. 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 time period for notification of the system administrator and the procedures established for updating the account status and preventing the employee from having unauthorized access to a user terminal.

Note: The period of time for notification of the system administrator is to be set such that it is unlikely that the terminated employee would gain access to a user terminal within the notification period.

37. 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 and time period for notification of the system administrator, and the procedures established for updating the account status and preventing the employee from having unauthorized remote access.

Note: The period of time for notification of the system administrator is to be set such that it is unlikely that the terminated employee would gain remote access within the notification period.

38. "User access listing" reports produced 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;

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- 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.

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

Note: MICS #38(e) applies to a review of the assigned functions for the selected user account with group membership.

Generic User Accounts

- 39. 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.
- 40. Generic user accounts at the application level are prohibited unless user access is restricted to inquiry only functions.

Service & Default Accounts

- 41. 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.

- 42. 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.
- 43. 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.

Backup and Recovery Procedures

- 44. 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).

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

c. Database contents and transaction logs.

45. 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: 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.

46. Backup system logs 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.
47. 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.
48. Annually, IT personnel test the recovery procedures.

Recordkeeping

49. System documentation for all in-use components of the interactive gaming system (versions of application, database, network hardware, and operating system) is maintained, including descriptions of both hardware and software (including version numbers), operator manuals, etc.
50. 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.
51. 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.
52. "User Access Listing" reports (requirements listed at MICS #33) for the interactive gaming system are to be retained for at least one day of each month for the most recent five years. The reports may be archived electronically if the listing is written to unalterable media (secured to preclude alteration). The list of users and user access for an interactive gaming system must be available in electronic format that can be analyzed by analytical tools (e.g., spreadsheet or database) that may be employed by Board agents.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

53. The IT department maintains current documentation with respect to the network topology (e.g., flowchart/diagram), deployment of server(s) housing application and database, 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

54. Reports and other documents/records may be directly written to an electronic document retention system in a portable document format (PDF) or scanned to an electronic document retention system into either a portable document format or standard image format provided that the system:
- a. Is properly configured to maintain the original version along with all subsequent versions reflecting all changes to the document;
 - b. Maintains a unique “hash” signature for each version of the document, including the original;
 - c. Retains and reports a complete log of changes to all documents including who (user ID and name) performed the changes and when (date and time);
 - d. Provides a method of complete indexing for easily locating and identifying the document including at least the following (which may be input by the user):
 - i. Date and time document was generated;
 - ii. Application or system generating the document;
 - iii. Title and description of the document;
 - iv. Name and title of the user/employee generating the document; and
 - v. Any other information that may be useful in identifying the document and its purpose.
 - e. Is configured to limit access to modify or add documents to the system through logical security of specific user accounts;
 - f. Is configured to provide a complete audit trail of all administrative user account activity.
55. If scanned, documentation must be verified by at least one additional person when being added to the electronic document storage system to ensure that the scanned version is identical to the original document. The second person must provide an electronic signature or other method of sign-off verification with the date and time to demonstrate the review was performed prior to the document being added to the system.
56. Electronic document retention systems may utilize CD-ROM, DVD-ROM, Hard Drive, or other type of storage, but the system must be properly secured through use of logical security measures (user accounts with appropriate access, proper levels of event logging, and document version control, etc.) and the system must be physically secured with all other critical components of interactive gaming system.
57. Electronic document retention systems must be equipped to prevent disruption of document availability and loss of data through hardware and software redundancy best practices, and backup processes.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

58. On a quarterly basis, accounting and audit personnel review at least 10% of the documentation added to the electronic document retention system to determine that:
- a. The documents are accurate reproductions of the original and the hash signatures match to the signatures recorded when the documents were added to the system;
 - b. The documents are readable and version control is functioning properly (i.e., all changes after the original was added are reflected in subsequent versions);
 - c. Indexing is correct (i.e., all information is accurate and the document is easily identified);
 - d. User access to add or modify documents is set to an appropriate level of access to administer the electronic document retention system, and no terminated employees have active user accounts on the system;
 - e. Event recording and reporting is functioning as designed and the logs are being reviewed by the appropriate personnel regularly; and
 - f. Redundancy exists and is adequately functional to limit the level of risk that an outage or loss of records may occur in the event of hardware failure or other unforeseen event.
59. Evidence of all reviews must be available upon request in accordance with Regulation 6.060.

Note: The written system of internal control pursuant to Regulation 6.090 must delineate the name and components of the electronic storage system and all procedures used for electronic document retention and delineate the titles for all employees responsible for administering and maintaining the system.

Production Environment Change Control Processes

60. The interactive gaming system operator must adopt a comprehensive and robust change control process to prevent unauthorized changes from being incorporated into the production environment at any layer. The process must include ALL changes to the interactive gaming production environment (operating system, network, databases, and applications). The change control process, including the titles of individuals responsible for all key decision points in the process, must be documented in the written system of internal control pursuant to Regulation 6.090. The change control process includes, at a minimum:
- a. Proposed changes to the production environment are evaluated sufficiently for the impact on all aspects of production environment and authorized by management personnel prior to implementation;
 - b. Proposed changes are properly and sufficiently tested prior to implementation into the production environment;
 - c. A strategy for reverting back to the last implementation (rollback plan) if the install is unsuccessful, including a test of the rollback plan prior to implementation to the production environment;
 - d. Sufficient documentation is maintained evidencing management evaluation, approvals, testing procedures and results, rollback plans, and any issues/resolutions encountered during implementation.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

61. All changes must be sufficiently documented, documentation must be maintained and include at a minimum:
 - a. The date the program was placed into service;
 - b. The nature of the change (if applicable);
 - c. 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
 - d. An indication of who performed all such procedures.
62. A copy of the associated equipment reporting form must be submitted to the Board pursuant to Regulation 14 for each new program or program change, and a record indicating Board approval must be maintained.
63. Quarterly, audit/accounting personnel review a sample of changes made during the prior period to determine that such changes were properly approved, adequately documented, properly tested, and issues resolved and rollback procedures applied. Evidence of the review must be maintained and available upon request.
64. If the interactive gaming system operator develops any software that interfaces with the interactive gaming application, or develops any or all source code for the interactive gaming application modules, then the operator must adopt and document in its system of internal control a comprehensive and robust software development change control process. The software development change control process must incorporate the following requirements:
 - a. Source code is maintained in a secured repository for code history and version control;
 - b. Technical documentation, including all regulatory submission and approval forms must be maintained and available upon request. Technical documentation must include approvals, development, testing, results of testing, and implementation into production. Documentation also includes a record of the final program or program changes, including evidence of user acceptance, date placed in service, programmer sign-off, and explanation of the changes;
 - c. The production environment is logically and physically segregated from the test/development environment(s);
 - d. All enhancements and changes are reviewed and approved by management prior to development and the review and approval process is documented. Review and approval documentation, along with technical documentation, is maintained by an individual independent of the development process;
 - e. Developers are precluded from having access to promote code changes into the production environment. All changes must be promoted into production by someone independent of the development and testing function;
 - f. End user documentation is maintained and remains current to reflect the most recent software changes. This documentation may be available electronically to the end user;
 - g. Adequate segregation of duties exists among developers, testing personnel, administrators, personnel who may promote changes into production, personnel who may access frozen code, etc.;

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- h. An evaluation of the impact of changes on all parts of the production environment and interactive gaming application is performed, and roll-back plan has been developed in case of failed promotion into production; and
- i. Analysis and verification processes are performed to establish the integrity of data when conversion or migration occurs as part of the development process.

General Operation of Interactive Gaming

- 65. All URL addresses, points of access, and communication media for remote interactive gaming operations conducted are to be delineated in the written system of internal control.
- 66. All compensation received by the operator of interactive gaming and/or the interactive gaming service provider resulting from interactive gaming and reported as gross revenue pursuant to Regulation 5A.170 is deposited into a segregated, separate bank account.
- 67. The compensation amount collected by the operator of interactive gaming as gross revenue pursuant to Regulation 5A.170 is calculated for each 24-hour day. The term "gaming day" as used in these MICS refers to an interval of 24 hours as defined by the operator of interactive gaming. The operator's end time of a gaming day is delineated within the written system of internal control pursuant to Regulation 6.090.
- 68. The operator shall establish procedures to reasonably ensure that credit is not extended to an authorized player and that the deposit of funds derived from the extension of credit by affiliates or agents of the operator into a patron's interactive gaming account is prevented. Such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.
- 69. The operator shall establish procedures to reasonably ensure that funds deposited into an interactive gaming account from a financial institution shall not be transferred out of the interactive gaming account to a different financial institution. Such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.
- 70. Procedures are established to ensure an authorized player has sufficient available funds prior to processing the authorized player's wagering transaction.

Casino Account Transfers

Note: A "casino account" is defined as a player's funds on deposit in any safekeeping, front money or wagering account being maintained at a gaming establishment operated by the of the operator of interactive gaming.

- 71. A transfer of funds between an authorized player's interactive gaming account and the player's casino account (i.e., to and from a player's casino account) is to be transacted through a Board-approved mechanism designed to facilitate electronic commerce transactions.
- 72. A transfer transaction between an interactive gaming account and a casino account is to be recorded in the "daily interactive gaming player's funds transactions report" (refer to MICS #127).
- 73. A transfer document is prepared and maintained which includes:
 - a. Authorized player's name, casino account number and interactive gaming account number;
 - b. Date of transfer;
 - c. Type of transfer (deposit/withdrawal to/from casino account);

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- d. Dollar amount of transfer;
- e. Method used by authorized player to approve transfer, if not in-person;
- f. Signature of authorized player, if in-person; and
- g. Signature of employee handling the transaction.

Registering Authorized Players

- 74. The operator shall establish procedures to create a patron's interactive gaming account pursuant to the requirements of Regulation 5A.110. Such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.
- 75. The information obtained to create an authorized player's interactive gaming account is recorded and maintained. The information includes:
 - a. Authorized player's name, authorized player's fictitious name(s) to be used while engaged in interactive gaming (if applicable), and current residential address;
 - b. Authorized player's date of birth;
 - c. Authorized player's e-mail address;
 - d. Type of identification credential, the last four digits of the relevant credential number, expiration date of credential, and date credential was examined; and
 - e. Source used to verify the accuracy of the information provided.

Identification and Verification of Authorized Players

- 76. The operator shall establish procedures to verify the identity and age of a player to ensure the player is authorized to engage in interactive gaming. Such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.

Note: The procedures are to involve robust and redundant identification methods to mitigate the risks of non face-to-face transactions inherent in interactive gaming.

Protection of the Interactive Gaming Accounts

- 77. An authorized player may hold only one interactive gaming account with the operator of interactive gaming.
- 78. An interactive gaming account cannot be set up with an anonymous or fictitious name, but may be associated with one or more fictitious "screen names" to be used while engaging in interactive gaming provided that the operator complies with MICS #75(a).
- 79. The interactive gaming written system of internal control pursuant to Regulation 6.090 is to delineate:
 - a. Procedures established for the use of a payment processor to allow the operator of interactive gaming to fund an authorized player's interactive gaming account;
 - b. The deposit methods available to authorized players to fund accounts and a complete description of the entire process for each deposit method, including situations where additional information must be requested prior to completing the deposit transaction; and

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- c. Procedures performed to ensure that wagering transactions do not cause an authorized player's wagering account balance to fall below zero.
80. The routing procedures for deposits by mail (e.g., checks, cashier's checks, or money orders) require that the mail deposits are received by a department independent of the interactive gaming department.
81. Interactive gaming account deposits received via mail are documented on a listing indicating the following:
- a. Authorized player's name on account to which the deposit is being applied and the name of individual making the deposit (if made by other than the authorized player);
 - b. Amount of deposit;
 - c. Nature of deposit (if other than a check); and
 - d. Date payment was received.
82. Direct access to an active authorized player's interactive gaming account to withdraw funds is restricted to the authorized player who owns the interactive gaming account and who is confirmed to be the owner by using positive authorized player identification methods such as a PIN number or password.
83. Indirect access (i.e., authorized player is not providing a PIN number or password) to an active authorized player's interactive gaming account to withdraw funds involves assisted access by an employee of the operator of interactive gaming whether online or by other means. The employee who is assisting with an indirect access is to use challenge questions to identify the person making remote access or employ a sufficient alternative process to ensure that the person is accurately identified as the owner of the interactive gaming account. If challenge questions are used, the responses to challenge questions should be obtained during the registration process for a player interactive gaming account. Such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.
84. An authorized player's request for withdrawal of funds is completed by the operator of interactive gaming within five days, unless there is a pending unresolved player dispute or investigation.
85. For withdrawals, a transfer of funds from an authorized player's interactive gaming account to an account with a financial institution is to be made to an account in the name of the authorized player. If a check is used as payment for a withdrawal of funds, the check is to be made payable to the authorized player and forwarded to the authorized player's address on file.
86. Documentation of withdrawal is prepared and maintained. The withdrawal document contains the following information:
- a. Authorized player's name and account number;
 - b. Date of withdrawal;
 - c. Dollar amount of withdrawal;
 - d. Method of withdrawal (e.g., check, wire transfer, cash, etc.); and
 - e. Signature of employee handling the withdrawal transaction.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

87. Addition or removal of monies from an interactive gaming account other than an authorized player's deposit or withdrawal must be sufficiently recorded (including substantiation of reasons for increases/decreases) and authorized/performed by supervisory personnel. Job title of supervisory personnel is delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090. The "daily interactive gaming account balance adjustment report" is randomly verified by accounting/audit personnel on a quarterly basis.
88. Changes to an authorized player's password are performed in a manner that ensures that the change is properly authorized by the authorized player. If e-mail is a component of this process, the procedures for the secure use of e-mail as a medium for communicating secure information must be documented in the licensee's written policies. The licensee shall develop alternative procedures for use in the event that an authorized player no longer has access to the e-mail address of record. The written system of internal control pursuant to Regulation 6.090 shall delineate the title of the person responsible for the documentation of these procedures.
89. Any change made to an interactive gaming account requires notification to the authorized player through e-mail, mail or other method to reasonably ensure the authorized player has been properly notified.
90. The operator shall document in the written system of internal control pursuant to Regulation 6.090 a description of procedures used to ensure full compliance with the reserve requirements of Regulation 5A.125 and to ensure prompt availability of patron funds for authorized withdrawals.
91. Funds in authorized players' interactive gaming accounts may not be used as security by the operator of interactive gaming and/or the interactive gaming service provider for any financial transactions.
92. Winnings awarded to players are posted immediately to the appropriate player's interactive gaming account at the completion of the game.
93. An authorized player shall not transfer funds to any other authorized player.

Interactive Gaming Engaged between Human Individuals

94. The operator shall establish procedures to reasonably ensure interactive gaming is conducted only between human individuals. Such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.

Responsible Interactive Gaming

95. The operator shall establish procedures to promote responsible interactive gaming. Such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.
96. The operator's website is to provide information and/or a link to information on player protection and responsible gaming.
97. The operator shall establish procedures to allow authorized players the option, through their interactive gaming account, to set specified limits (e.g., wager limit, loss limit, time-based loss limits, deposit limit, session time limit and time-based exclusion from gambling) and/or an option to "self-exclude" in the interactive gaming system and such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.
98. The operator shall establish procedures to comply with the requirements of Regulation 5A.130 regarding self-exclusion and such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

99. The operator shall establish procedures to reasonably ensure a player under the age of 21 is prohibited from participating in interactive gaming and such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.

Protection of Authorized Player's Personally Identifiable Information

100. The operator shall establish procedures and policies to protect the authorized player's personally identifiable information consistent with the requirements specified in Regulation 5A.070(9). Such procedures and policies are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.
101. The designation of senior company official(s) with primary responsibility for the design, implementation and ongoing evaluation of the procedures related to the protection of the authorized player's personally identifiable information is delineated in the written system of internal control pursuant to Regulation 6.090. If more than one senior company official is designated, then the responsibilities assigned to each official are to be specified in the system.

Closed/Inactive Accounts

102. The interactive gaming agreement approved by the chairman pursuant to Regulation 5A.120(12) indicates the operator's policy as to the time period without player activity in determining when an interactive gaming account shall be deemed dormant. Furthermore, the agreement indicates the operator's process for notifying an authorized player prior to the closing of the account and handling of abandoned funds.

Note: Only the language/form of the agreement, or change thereto, is to be approved. The operator is not required to have each agreement approved separately, provided that the agreement with each player is identical.

103. Every interactive gaming agreement between an operator of interactive gaming and any authorized player is to be maintained and made available for inspection by Board agents.
104. A monthly "closed/inactive interactive gaming accounts report" is prepared and maintained indicating the interactive gaming accounts which were closed and not available for an authorized player to access for wagering transactions. Access to closed/inactive interactive gaming account information is restricted to those positions which require access and are so authorized by management. Such access is to be delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090. The report is to include, at a minimum:
- a. The authorized player's name and account number;
 - b. User ID and name of employee handling the closure of account;
 - c. Date and time account was opened;
 - d. Last date authorized player logged into account;
 - e. Number of days since authorized player logged into account;
 - f. Date and time account was closed; and
 - g. Balance of account when closed.
105. An authorized player will need to establish a new interactive gaming account once a prior interactive gaming account has been closed.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

Authorized Player Disputes

106. The operator shall establish procedures to handle disputes with authorized players. Such procedures are delineated within the interactive gaming written system of internal control pursuant to Regulation 6.090.

Contests/Tournaments

107. A player is to register prior to being allowed to participate in an interactive gaming contest/tournament and the player is to provide the following information:

- a. Player's name;
- b. Player's date of birth;
- c. State or foreign jurisdiction; and
- d. E-mail address.

108. Procedures are to be performed to verify that a player registering to participate in an interactive gaming contest/tournament is 21 years of age or older and resides in a jurisdiction that has no prohibitions against a registered player from engaging in interactive gaming contests/tournaments.

109. Interactive gaming contest/tournament rules are available to a registered player on the website where the interactive gaming contest/tournament is being conducted. The rules must include at a minimum:

- a. All conditions registered players must meet to qualify for entry into, and advancement through, the contest/tournament.
- b. Specific information pertaining to any single contest/tournament, including the dollar amount of money placed in the prize pool.
- c. The distribution of funds based on specific outcomes.
- d. The name of the organization (or persons) registered pursuant to NRS 463.169 that conducted the contest/tournament on behalf of, or in conjunction with, the licensee if applicable.

110. Procedures are performed to verify that interactive gaming contest/tournament awards are paid to a registered player who is 21 years of age or older.

111. The contest/tournament entry fees and payouts are summarized and posted to the accounting records on at least a monthly basis.

112. The results of each contest/tournament are recorded and available on the operator of interactive gaming's website for the participants to review. The recording includes the name of the event, date(s) of event, total number of entries, dollar amount of entry fees, total prize pool, and the dollar amount paid for each winning category. The name of each winner is recorded and maintained but not made available to the participants unless authorized by management personnel. Two employees, one of whom is independent of the collection of entry fees, reconcile the total amount of issuance for the contest/tournament in exchange for entry fees to the final amount at the end of the contest/tournament. The reconciliation is documented and signed by the employees.

Note: For free contests/tournaments (i.e., registered player does not pay an entry fee), the information required by the above MICS must be recorded except for the number of entries, dollar amount of entry fees and total prize pool.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

113. For interactive gaming contest/tournament prize pools where the amount of the pool is determined through registered player contributions from poker pots, the daily contributions and the total contributions are recorded in the "interactive gaming contest/tournament report".

114. The aforementioned interactive gaming contest/tournament records are maintained for each event.

Promotional Progressive Pots and Pools

Note 1: Promotional progressive pots and pools are defined as pots and pools which are contributed to by authorized players and distributed back to authorized players based upon the occurrence of a predetermined event.

Note 2: A promotional pot or pool is to be handled in accordance with Regulation 5A.145.

115. The dollar amount of funds contributed by authorized players into the pools is returned when won in accordance with the posted rules with no commission or administrative fee withheld.

Note 1: The payout may be in the form of personal property (e.g., car).

Note 2: A combination of a promotion and progressive pool may be offered.

116. The conditions for participating in promotional progressive pots, pools, and any other promotion including those as a result of drawings and giveaway programs are available to a registered player on the website where the interactive gaming promotion is being conducted.

117. Rules governing promotional progressive pools are available to a registered player on the website where the interactive gaming promotional progressive pool is being conducted, and designate:

- a. The amount of funds to be contributed from each pot;
- b. What type of hand it takes to win the pool (e.g., what constitutes a "bad beat");
- c. The percentages used to calculate the payout amounts;
- d. How/when the contributed funds are added to the pools; and
- e. Amount/percentage of funds allocated to primary and secondary (reset) pools, if applicable.

118. The dollar amount of promotional progressive pots, pools, and any other promotion must be conspicuously displayed on the website where the interactive gaming promotional progressive pool is being conducted. At least once a day, the progressive amount displayed on the website, if applicable, is increased based upon the amount of funds to be contributed to the promotional progressive pots, pools, and any other promotion.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

Authorized Player Promotional Account

Note 1: Compliance with MICS #119 - #123 is required only for authorized player promotional accounts that accumulate points that are subsequently redeemed by the authorized player for cash, merchandise, etc. These MICS do not apply to player rating only systems (i.e., the evaluation of an authorized player's wagering activity and the choice and/or dollar amount of complimentary provided to an authorized player are solely the result of an employee's judgment).

Note 2: As used in these Interactive Gaming MICS, the term "point" or "points" is a generic term and refers to a representative of value awarded to an authorized player based upon specific criteria established by the operator of interactive gaming. Commonly, points are earned by an authorized player placing wagers or any other specified criterion. Authorized player promotional accounts are used to track points earned/awarded to authorized players.

119. The addition/deletion of points to player promotional accounts other than through an automated process related to actual play must be sufficiently recorded (including substantiation of reasons for increases) in the "interactive gaming authorized player promotional account balance adjustment report" and authorized/performed by supervisory personnel of the player promotions, or interactive gaming department. The "interactive gaming authorized player promotional account balance adjustment report" is randomly verified by accounting/audit personnel on a quarterly basis.

Note: The above MICS does not apply to the deletion of points related to inactive or closed accounts through an automated process.

120. Employees who redeem points for patrons cannot have access to inactive or closed accounts without supervisory personnel authorization. Documentation of such access and approval is created and maintained.

121. Changes to the player promotional account parameters, such as point structures and employee access, must be performed by supervisory personnel independent of the interactive gaming department. Alternatively, changes to player promotional account parameters may be performed by interactive gaming supervisory personnel if sufficient documentation is generated and the propriety of the changes is randomly verified by personnel independent of the interactivity gaming department on a quarterly basis.

122. All other changes to the player promotional account must be appropriately documented.

123. Rules and policies for player promotional accounts including the awarding, redeeming and expiration of points are available to a registered player on the website where the interactive gaming player promotional activity is being conducted.

Documentation

124. An "interactive gaming account transaction detail report" is to be created on demand, and at least daily, indicating by authorized player the detailed, sequential activity as follows:

- a. Date of activity;
- b. Authorized player's name and account number;
- c. Date and time authorized player session started;
- d. State or foreign jurisdiction where authorized player is located while logged into session;
- e. Unique transaction number;

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- f. Game session number, if transfer to/from game;
 - g. Date and time of each transaction;
 - h. Amount of each transaction;
 - i. Type of each transaction (e.g., deposit, withdrawal, transfer to game, transfer from game, adjustment, etc.);
 - j. Name of authorized player's financial institution and last four digits of account number for deposit and withdrawal transactions, if applicable;
 - k. Method of deposit/withdrawal (e.g., cash, debit or credit card, personal check, cashier's check, wire transfer, money order and transfer to/from casino account);
 - l. User ID and employee name handling the transaction, if assisting authorized player;
 - m. Amount of outstanding account balance before and after each transaction;
 - n. Date and time authorized player session ended;
 - o. Subtotals by transaction type; and
 - p. Ending account balance at the end of the authorized player's session.
125. An "interactive gaming account transaction detail report" is to be maintained:
- a. For authorized players through on-line access to their interactive gaming account, at a minimum, for the prior 180-day period.
 - b. For authorized players through off-line access to interactive gaming account records, at a minimum, for the prior five-year period.
126. An "interactive gaming account balance summary report" is to be created on demand, and at least daily, indicating by authorized player with an account balance the following information:
- a. Date of activity;
 - b. Authorized player's name and account number;
 - c. Date account was opened;
 - d. Date of last activity;
 - e. Amount of beginning account balance;
 - f. Total amount of deposit transactions;
 - g. Total amount of withdrawal transactions;
 - h. Total amount of account adjustment transactions;
 - i. Total amount of transfers to game;
 - j. Total amount of transfers from game; and

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- k. Amount of ending account balance.
127. A “daily interactive gaming player’s funds transactions report” is prepared and maintained indicating by authorized player the deposit/withdrawal/adjustment transactions to a player’s interactive gaming account that includes:
- a. Authorized player’s name and account number;
 - b. Amount of beginning account balance;
 - c. Unique transaction number;
 - d. Date and time of deposit/withdrawal or account balance adjustment;
 - e. Amount of deposit/withdrawal or account balance adjustment;
 - f. Nature of deposit/withdrawal (e.g., cash, debit or credit card, personal check, cashier’s check, wire transfer, money order and transfer to/from casino account);
 - g. Reason/description of adjustment to account balance, if applicable;
 - h. User ID and name of employee handling the deposit, withdrawal or account balance adjustment transaction, if assisting authorized player;
 - i. User ID and name of supervisor authorizing an adjustment to account balance, if applicable;
 - j. Totals for each type of transaction; and
 - k. Amount of ending balance.
128. A “daily interactive gaming account balance adjustment report” is prepared and maintained indicating by authorized player adjustment transactions to a player’s interactive gaming account that includes:
- a. Authorized player’s name and account number;
 - b. Date and time of account balance adjustment;
 - c. Unique transaction number;
 - d. User ID and name of employee handling the account balance adjustment transaction;
 - e. User ID and name of supervisor authorizing an adjustment to account balance;
 - f. Amount of account balance adjustment;
 - g. Type of account adjustment; and
 - h. Reason/description of adjustment to account balance.
129. An “interactive gaming game play report” by game type is maintained by day with cumulative month-to-date and cumulative year-to-date totals and includes the following information:
- a. Date of activity;
 - b. Game type;

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- c. Date and time game started;
 - d. Date and time for each game transaction;
 - e. Type of game transaction;
 - f. Amount of game transaction;
 - g. Contribution amount to jackpot pool or progressive, if applicable;
 - h. Compensation amount collected by operator of interactive gaming as gross revenue pursuant to Regulation 5A.170;
 - i. Compensation amount collected by authorized player and state or foreign jurisdiction, if applicable for taxation purposes;
 - j. Game result;
 - k. Amount of jackpot win, if applicable;
 - l. Date and time game ended;
 - m. Winning authorized player's name and account number;
 - n. Win amount deposited to authorized player's account; and
 - o. Total amount by transaction type.
130. An "interactive gaming revenue report" by type of game that is maintained by day, with cumulative month-to-date and cumulative year-to-date totals and includes the following information:
- a. Date;
 - b. Type of game;
 - c. Total wagered;
 - d. Total amount contributed to the progressive pool, if applicable;
 - e. Compensation amount collected by operator of interactive gaming pursuant to Regulation 5A.170;
 - f. Other amounts collected by operator of interactive gaming;
 - g. Description of other amounts collected;
 - h. Amounts refunded; and
 - i. Description of amounts refunded.
131. An "interactive gaming contest/tournament report" is prepared and maintained for each contest/tournament conducted which includes, at a minimum:
- a. Date of activity;
 - b. Name of contest/tournament;

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

- c. Name of each authorized player participating , amount of entry fee paid, and date paid;
 - d. Total amount of entry fees collected;
 - e. Name of each winning authorized player, amount paid to winner, and date paid;
 - f. Total amount of winnings paid to authorized players; and
 - g. Compensation amount collected by the operator of interactive gaming.
132. A monthly “interactive gaming revenue deposit report” is prepared and maintained by day, with cumulative month-to-date and cumulative year-to date totals which includes:
- a. Month/year of activity;
 - b. Bank account number;
 - c. Date of deposit; and
 - d. Amount of gaming day deposit for compensation collected from operation of interactive gaming as gross revenue pursuant to Regulation 5A.170.
133. An “interactive gaming daily progressive pool activity report” is prepared and maintained which includes:
- a. Progressive pool name;
 - b. Beginning balance;
 - c. Total wagers by game type;
 - d. Contributions to primary pool;
 - e. Contributions by hidden/secondary pool, as applicable;
 - f. Date and time of payout;
 - g. Winning authorized player(s) name and account number;
 - h. Payout amount(s);
 - i. User ID and name of the employee handling the payment, if applicable;
 - j. Progressive reset amount after payout;
 - k. User ID and name of employee performing an adjustment to the pool amount for other than an authorized player winning the pool amount during game play;
 - l. Reason/description for employee making an adjustment to the pool amount;
 - m. Date and time of pool amount adjustment; and
 - n. Ending balance.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

134. An “interactive gaming authorized player promotional account summary report” is prepared and maintained which includes:
- a. Authorized player’s name and account number;
 - b. Beginning balance by promotion type;
 - c. Total amount of awards by type;
 - d. Total amount used by type;
 - e. Total amount expired by type;
 - f. Total adjustment amount by type; and
 - g. Ending balance by promotion type.
135. An “interactive gaming authorized player promotional account daily activity report” is prepared and maintained by authorized player which includes, at a minimum:
- a. Authorized player’s name and account number;
 - b. Date and time of activity;
 - c. Activity type (usage, award, expired, adjusted, etc.);
 - d. Game type, if applicable;
 - e. Amount; and
 - f. Subtotals by activity type.
136. An “interactive gaming authorized player promotional account balance adjustment report” is prepared and maintained by authorized player which includes, at a minimum:
- a. Authorized player’s name and account number;
 - b. Date and time of adjustment;
 - c. User ID and name of employee performing the adjustment;
 - d. User ID and name of supervisor authorizing the adjustment;
 - e. Amount of adjustment; and
 - f. Reason/description of adjustment.
137. A monthly “interactive gaming revenue recap report” is prepared and maintained which includes the daily and month-to-date interactive gaming revenue (pursuant to Regulation 5A.170). Additionally, the monthly “interactive gaming revenue recap report” shows a reconciliation of the taxable interactive gaming revenue from the month-end “interactive gaming revenue report” to the monthly total interactive gaming revenue amount reported on the NGC tax return. Any adjustment to the revenue amount indicated in the “interactive gaming revenue recap report”, with supporting documents, may need to be reflected in this reconciliation.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

Accounting/Audit Standards

138. The interactive gaming audit is conducted by someone independent of the interactive gaming operations.
139. Daily, audit/accounting personnel are to use the "interactive gaming daily progressive pool activity report" to reconcile the amount indicated on the payout amount displayed to the authorized player to the amount received from interactive gaming play and the payouts made for each promotional progressive pot and/or pool. This reconciliation must be sufficiently documented (including substantiation of differences, adjustments, etc.)
140. Daily, accounting/audit personnel perform the following procedures using the reports provided by the interactive gaming system:
- a. For a sample of games, verify the accuracy of the compensation amount indicated on the "interactive gaming game play report" that resulted from wagering activity.
 - b. Trace the total daily compensation amount indicated on the "interactive gaming game play report" to the compensation amount indicated on the "interactive gaming revenue report".
 - c. Trace the total daily compensation amount indicated on the "interactive gaming revenue report" to the monthly "interactive gaming revenue deposit report".
 - d. Reconcile the total amount of interactive gaming account deposit, withdrawal and account adjustments transactions indicated in the "interactive gaming account balance summary report" to the amount recorded in the "interactive gaming player's funds transactions report".
 - e. Review the interactive gaming system's exception reports for propriety of transactions and unusual occurrences. All noted improper transactions or unusual occurrences are investigated with the results documented.
141. At least annually, the interactive gaming system is reviewed by personnel independent of the individual who sets up or makes changes to the system parameters. The review is performed to determine that the configuration parameters are accurate and have not been altered without appropriate management authorization (e.g., verify the accuracy of the compensation % or flat rate to collect on wagering activity). The test results are documented and maintained.
142. At least monthly, reconcile the dollar amount of the compensation collected and deposited as recorded in the monthly "interactive gaming revenue deposit report" to the dollar amount indicated in the bank account records.
143. At least monthly, reconcile the total outstanding balance of interactive gaming accounts indicated in the "interactive gaming account balance summary report" to the dollar amount indicated in the bank account records.
144. At least monthly, review the "interactive gaming account balance summary report" to verify that a negative account balance does not exist, or if it exists, was not the result of wagering transactions having been permitted in excess of the patron's account balance.
145. For one day each month, accounting/audit personnel reconcile the total amount of the listing of interactive gaming account deposits received via mail, if required to be prepared, with the deposit amount indicated in the bank account records.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

146. For all interactive gaming contests/tournaments and promotional payouts (including payouts from computerized player promotional accounts) conducted on the operator of interactive gaming's website, the following documentation is to be maintained:
- a. Copies of the information provided on the website to the registered players describing the contests, tournaments, promotional payouts, drawings, and giveaway programs;
 - b. Effective dates;
 - c. Accounting treatment, including general ledger accounts, if applicable;
 - d. For interactive gaming tournaments and contests, a list of the registered players along with the information required to be obtained pursuant to MICS #107; and
 - e. For interactive gaming tournaments and contests, the name of the organization (or person) registered pursuant to NRS 463.169 that conducted the contest/tournament on behalf of, or in conjunction with, the operator of interactive gaming, if any. The extent of responsibilities (including MICS compliance responsibilities) each organization and the operator of interactive gaming had in the contest/tournament (e.g., ABC company is to receive 100% of the entry fees and provide noncash prizes to the winners with the operator of interactive gaming collecting entry fees, dealing the tournament and distributing prizes to winners) will also be documented.
147. When payment is made to the winners of an interactive gaming contest/tournament, accounting/audit personnel will review the appropriate "interactive gaming contest/tournament report" to determine whether, based on the entry fees collected, the payouts made and the amounts withheld by the operator of interactive gaming, if applicable, were distributed in accordance with the contest/tournament rules.
148. On a daily basis, audit/accounting personnel reconcile the progressive amount displayed on the website where the interactive gaming promotional progressive pool is being conducted to the amount indicated in the "interactive gaming daily progressive pool activity report". This reconciliation must be sufficiently documented (including substantiation of differences, adjustments, etc.)
149. Monthly, accounting/audit personnel review all payouts for the promotional progressive pots, pools, or other promotions to determine proper accounting treatment and proper interactive gaming revenue win/loss computation.
150. Monthly, accounting/audit personnel perform procedures to reasonably ensure that payouts for the promotional progressive pots, pools, or other promotions are conducted in accordance with conditions provided to the patrons. The procedures must include a review of documents along with employee interviews and/or observations.
151. For player promotional accounts, an accounting/audit employee shall perform the following procedures at least one day per quarter:
- a. Review the "interactive gaming authorized player promotional account balance adjustment report" for all point addition/deletion, other than for point additions/deletions made through an automated process, for propriety.
 - b. Review exception reports including transfers between accounts.
 - c. Review documentation related to access to inactive and closed accounts.

STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INTERACTIVE GAMING

152. At least annually, the computerized interactive gaming player promotional account system is reviewed by personnel independent of the individuals who set up or make changes to the system parameters. The review is performed to determine that the configuration parameters are accurate and have not been altered without appropriate management authorization (e.g., verify the accuracy of the awarding of points based on the dollar amount wagered). The system should also be tested, if possible, to further verify the accuracy of the configuration parameters (e.g., simulate activity to verify the accuracy of the amount of points awarded). The test results are documented and maintained.
153. At least one day per calendar quarter, the “interactive gaming account balance summary report” is reviewed, for Regulation 5A.125 compliance purposes, to ensure that the amount of the reserve being maintained is equal to the sum of all authorized players’ funds held in the interactive gaming accounts.
154. Documentation (e.g., log, checklist, notation on reports, and tapes attached to original documents) is maintained evidencing the performance of interactive gaming audit procedures, the exceptions noted and follow-up of all interactive gaming audit exceptions.