NEVADA GAMING CONTROL BOARD
INTERNAL CONTROL PROCEDURES

INFORMATION TECHNOLOGY

Note 1: For any Nevada Gaming Control Board ("Board") authorized computer applications, alternate documentation and/or procedures which provide at least the level of control described by these Internal Control Procedures ("ICP" or "ICPs") as determined by the Tax and License Division will be acceptable, and an ICP variation pursuant to Regulation 6.100 will be unnecessary.

Note 2: Unless otherwise specified, all Information Technology ("IT") ICPs 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 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 ("operator"), the entertainment tax related application being used by such operator to report entertainment revenue must be compliant with the ICPs.

Note 3: These ICPs do not apply when an IT service provider (including an affiliate of an operator) is engaged by a licensee/operator to operate an entertainment tax related application/system (box office system or point-of-sale ("POS") system) for handling and recording live entertainment taxable admission sales. To further clarify, these ICPs do not apply when:

a. The licensee/operator has only installed the user terminals to record live entertainment taxable admission and to print the related reports for the recorded sales; and

b. The administrative functions for the computerized box office system or POS are being performed by an IT service provider.

Note 4: If an IT service provider is used for gaming and entertainment tax related applications, including the underlying databases and operating systems, the licensee is ultimately responsible for the proper design and implementation of the procedures required to meet all applicable ICPs, regardless of who is performing the IT function.

Note 5: These ICPs do not apply to the licensee's use of a Nevada Gaming Control Board ("Board") approved pari-mutuel system.

Note 6: Licensees performing or utilizing the following function(s) are required to be in compliance with the applicable Minimum Internal Control Standards ("MICS"), pursuant to Regulation 6.090, related to each specific item(s): any changes to the production environment, any in-house software development, any modifications to purchased software programs, and the use of wagering accounts pursuant to Regulation 5.225.

Note 7: Definitions. The following terminology and respective definitions are used in these ICPs unless the context requires otherwise:

"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. User accounts established by/for, and used by manufacturers of the system for vendor support purposes are not considered to be generic accounts.

"Group membership" (group profile) is a method of organizing user accounts into a single unit (by job position), which access to application functions can be modified at the unit level and the changes take effect for all user accounts assigned to the unit. A user account can be assigned to one or more groups.

"Hosting center" is a remote facility where Board regulated hardware or software is located. The hosting center must be registered with the Board, pursuant to Regulation 5.230.

"IT personnel" are employees of the licensee/operator, or an IT service provider, 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. The term is not limited to personnel within an IT department, provided that the employee has sufficient training and knowledge.

"IT service provider" is a person engaged by the licensee to provide system management, system administration, user access administration, support, security, and/or disaster recovery service.

"Service accounts" are accounts which automated system functions (services) are dependent to execute. A service account does not correspond to an actual person. These are often built-in accounts that an automated system function uses to access resources needed in order to perform activities; however, some automated functions require actual user accounts to perform certain functions, and can be employed using domain accounts to run functions.

"System administrator" is the individual(s) responsible for maintaining the stable operation of the IT environment (including software and hardware infrastructure and application software) and/or has system authorization/access to perform the following administrative function(s):

a. Add, change, or delete user accounts and associated user provisioning for database, operating system, and network layers (can also include user access administrator function for an application layer);

b. Modify operating system, database, and application security and policy parameters;

c. Add, change, or delete system exception logging information; or

d. Add, change, or delete permissions to data files and folders.

Note: If there is no IT department, the system administrator must be an authorized employee who does not have access to gaming and entertainment systems.

"User access administrator" is the individual(s) responsible for and has system authorization/access to add, change, or delete user accounts and associated user provisioning. User provisioning consists of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties.

"Vendor supported system" is one type of critical IT systems and equipment where the source code is supported solely by the manufacturer of such system. The manufacturer support of source code does not include performing the function of a system administrator or a user access administrator when the system is in use by the licensee.

Physical Access and Maintenance Controls

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

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

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

   b. Adequate security mechanisms, such as traditional key locks, biometrics, combination door locks, or an electronic key card system, to prevent unauthorized physical access to areas housing critical IT systems and equipment.

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

2. Access to areas housing critical IT systems and equipment, excluding vendor supported systems, is restricted to IT/authorized personnel. Gaming and entertainment department/area personnel, including the manufacturers of the IT equipment, are only allowed access to the areas housing critical IT systems and equipment for, excluding vendor supported systems, when authorized by IT/authorized personnel and with periodic monitoring by IT/authorized personnel during each access.

3. A record of each access described in ICP #2 by non-IT/authorized personnel is maintained and includes at a minimum:

   a. The name of the visitor(s);

   b. Date and time of arrival;

   c. Date and time of departure;

d. Reason for visit; and

e. The name of IT/authorized personnel authorizing such access.

4. Access to an area housing a vendor supported system is restricted to authorized IT/authorized personnel, or by system manufacturer personnel when authorized by management and with periodic monitoring during each access by IT/authorized personnel, or personnel independent of the department/area using such application.

5. A record of each access described in ICP #4, by system manufacturer personnel, is maintained and includes at a minimum:

   a. The name of the visitor(s);

   b. Date and time of arrival;

   c. Date and time of departure; and

   d. Reason for visit.

System Parameters

6. The computer systems, including gaming and entertainment applications, are secured through the use of passwords, biometrics, or other means approved by the Board. Security parameters for passwords, if configurable, must 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: uppercase letters, lowercase letters, numbers, and/or special characters;

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

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

   Note: ICP #6 does not apply to service accounts or generic accounts.

7. Exception reports (for application level only), if capable of being produced by the system (e.g., changes to system parameters, corrections, overrides, voids, etc.), are maintained.

User Accounts

8. Management personnel approves 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.

9. Provisioning of user accounts for personnel who transfer to a new department are performed or approved by management personnel, or persons independent of the department/area being

controlled. Any previously assigned application function access for the employee's user account is changed to inactive (disabled) prior to the employee accessing the new user account functions for the role or position in a new department/area.

10. User access listings include, if capable of being produced by the system, at a minimum:

    a. Employee's name and title or position;

    b. User login name;

    c. Full list and description of application functions that each group or user account can 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 or deactivated; and

    h. Group membership of user account, if applicable.

    Note: The user access listing is not required for entertainment tax related applications.

11. When multiple user accounts for one employee per application are used, only one user account can be active (enabled) at a time, if the concurrent use of the multiple accounts creates a segregation of duties deficiency. Additionally, the user account has a unique prefix/suffix to identify users with multiple user accounts within one application.

12. The system administrator (as applicable) is notified within a week, when an employee is known to be no longer employed (i.e., 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 within two weeks of notification.

13. The system administrator, as applicable, 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 (i.e., voluntary or involuntary termination of employment). Upon notification the system administrator changes the status of an employee's user account from active to inactive (disabled) status within a reasonable period of time, established by management.

14. User access listings, 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% of the users included in the listing. Documentation is maintained, which includes the identified accounts reviewed, documentation of the results of the review, e-mails or signatures, and dates indicating when the user access listing was reviewed. For each of the users, determine the following:

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 employee's user accounts have been changed to inactive (disabled) status within the required time period by ICPs #12 - #13;

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 ICP #6(a).

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

Note 1: ICP #14(e) applies to a review of the assigned functions for the selected user account with group membership.

Note 2: The required review of user access listings does not apply to user access listings for any entertainment tax related applications.

Note 3: The review applies to user access listings for computerized gaming systems with the following capabilities:

a. Generates reports identifying gaming revenues;

b. Generates detailed records of all markers, returned checks, or other similar credit instruments;

c. Generates statistical gaming records required by these ICPs; or

d. Generates any other records required by these ICPs.

Generic User Accounts

15. Generic user accounts at the operating system level, if used, are configured such that:

a. The user is automatically brought to the application login screen immediately upon logging into the operating system, and the user is logged out of the operating system automatically upon exiting the application; or

b. The user is only granted access to the assigned application(s) for the user's current job responsibilities, and the user is precluded from executing unassigned applications or functions from the terminal and is precluded from interactive access to the operating system through the proper security configurations.

16. 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 these ICPs.

Service and Default Accounts

17. Service accounts, if applicable, are utilized in a manner to prevent unauthorized and inappropriate usage to gain access to an application, the underlying databases, and the operating system. Service account login and password information is restricted to a limited number of authorized personnel.

    Note: Suggested methods include:

    a. Service accounts are configured such that the account cannot be used to directly login to the console of a server or workstation; or

    b. Service account passwords are to be changed at least once every 90 days, and immediately upon termination of system administrators.

18. Default accounts created upon installation of any operating system, database, or application are configured to minimize the possibility that these accounts can be utilized to gain unauthorized access to system resources and data.

19. Any other default accounts that are not administrator, service or guest accounts must 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.

Administrator Access

Note: "Administrator access" is access that would allow a user to:

a. Add, change, or delete user accounts and associated user provisioning;

b. Modify operating system, database, and application security and policy parameters;

c. Add, change, or delete system exception logging information; and

d. Add, change, or delete permissions to data files and folders.

20. Access to administer the network, operating system, applications, database security, and system parameters must be controlled in one of the following ways:

    a. Limited to authorized IT personnel under the supervision of management personnel of the licensee's/operator's IT department;

    b. If there is no IT department, limited to supervisory or management personnel independent of the department using the system and/or application; or

c. If there is no IT department, access may be granted to supervisory or management personnel that is not independent of the department using the system and/or application, provided that this access is reviewed and approved by supervisory or management personnel of a separate department. Documentation is created each time the administrator's access permissions change. This documentation must be signed by both the administrator and the personnel that approved the access permissions and must be maintained.

Backups

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

    a. Application data;

       Note: ICP #21(a) only applies if data files have been updated.

    b. Application executable files, unless such files can be reinstalled; and

    c. Database contents and transaction logs.

22. 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 can also be stored in the same building as the hardware/software, but not in the same immediate area, 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: ICP #22 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.

Recordkeeping

23. A list of all Board regulated systems (hardware and software) is maintained, which includes the system name and version identifier (indicating the period of time each version was in use). System documentation for all listed in-use versions of applications, databases, network hardware, and operating systems is maintained, including descriptions of hardware, software, and operator manuals, etc.

24. User access listings for all gaming systems are to be retained for at least one day per calendar quarter for the most recent five years. The lists can be archived electronically, if the listing is written to unalterable media (secured to preclude alteration).

    Note: User access listings do not need to be retained for entertainment related applications.

INFORMATION TECHNOLOGY

Electronic Storage of Documentation

25. Documents scanned or directly stored to unalterable media (secured to preclude alteration) must comply with the following conditions:

    a. The storage media contains the exact duplicate of the original document;

    b. All documents stored are maintained with a detailed index containing the gaming departments/areas and date in accordance with Regulation 6.040(1). This index is available upon Board request;

    c. Upon request by Board agents, hardware (e.g., terminal, printer, etc.) is provided in order to perform audit procedures;

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

    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.

26. If source documents and summary reports are stored on alterable storage media, the original documents and summary reports are retained.

Network Security and Data Protection

27. If guest networks are offered (e.g., networks that provide internet access for patrons, hotel guests, or vendors), adequate logical segregation is provided for guest networks 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.

28. Network shared drives containing application files and data for all Board regulated software are secured such that only authorized personnel can gain access.

29. Server consoles, and unattended user terminals in gaming areas (if configurable), are configured to automatically secure themselves after a period of inactivity elapses, the amount of time to be determined by management is not to exceed one minute. Users supply proper login credentials to regain access to the terminal or console.

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

Remote Access

31. For each computerized gaming or entertainment related application that can be accessed remotely for purposes of obtaining vendor support, prepare a log maintaining at a minimum:

a. Name or identifier of the licensee's/operator's employee authorizing access;

b. Name of manufacturer/vendor;

c. Name or identifier of manufacturer's/vendor's employee accessing the system;

d. Name of user account(s) which the vendor's employee accessed the system;

e. Name of system(s) accessed by the vendor;

f. Adequate and detailed description of work performed (including the old and new version numbers of any software that was modified); and

g. Date, time, and duration of access.

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

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

Data Access Control

Note: ICPs #34 - #36 apply to any Board approved gaming or entertainment related applications (including systems utilizing promotional accounts).

34. Procedures are in place to ensure that no alteration is permitted of any system stored transaction history or event log information that was properly communicated from the game, gaming device, or generated by the application.

35. Procedures are in place to ensure that all critical system stored data are non-alterable other than through normal operation processes. Critical system data includes data relating to, but not limited to, promotional accounts personal identification numbers and account balances and unpaid winning ticket information.

Note: Methods can include, but are not limited to, checksums on data tables or database encryption.

36. Procedures are in place to ensure that any communication with equipment or programs external to the approved system is performed through a Board approved secure interface. The documentation evidencing approval is maintained and available upon request.

Note: Documentation can include, but is not limited to, detailed network topology diagrams indicating all interfaces utilized to access Board approved systems by external programs.