§543.16 What are the minimum internal control standards for information technology?

(a) Physical security measures restricting access to agents, including vendors, must exist over the servers, including computer terminals, storage media, software and data files to prevent unauthorized access and loss of integrity of data and processing.

(b) Unauthorized individuals must be precluded from having access to the secured computer area(s).

(c) User controls.

(1) Computer systems, including application software, must be secured through the use of passwords or other approved means.

(2) Procedures must be established and implemented to ensure that management or independent agents assign and control access to computer system functions.

(3) Passwords must be controlled as follows unless otherwise addressed in the standards in this section.

(i) Each user must have his or her own individual user identification and password.

(ii) When an individual has multiple user profiles, only one user profile per application may be used at a time.

(iii) Passwords must be changed at least quarterly with changes documented. Documentation is not required if the system prompts users to change passwords and then denies access if the change is not completed.

~~(iv) The system must be updated to change the status of terminated users from active to inactive status within 72 hours of termination.~~

~~(v) At least quarterly, independent agents must review user access records for appropriate assignment of access and to ensure that terminated users do not have access to system functions.~~

~~(vi) Documentation of the quarterly user access review must be maintained.~~

~~(vii) System exception information (*e.g.*, changes to system parameters, corrections, overrides, voids, etc.) must be maintained.~~

~~(4) Procedures must be established and implemented to ensure access listings are maintained which include at a minimum:~~

~~(i) User name or identification number (or equivalent); and~~

~~(ii) Listing of functions the user can perform or equivalent means of identifying same.~~

~~(d) Adequate backup and recovery procedures must be in place that include:~~

~~(1) Daily backup of data files;~~

~~(i) Backup of all programs. Backup of programs is not required if the program can be reinstalled.~~

~~(ii) Secured storage of all backup data files and programs, or other adequate protection to prevent the permanent loss of any data.~~

~~(iii) Backup data files and programs may be stored in a secured manner in another building 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.

(2) Recovery procedures must be tested on a sample basis at least annually with documentation of results.

(e) Access records.

(1) Procedures must be established to ensure computer access records, if capable of being generated by the computer system, are reviewed for propriety for the following at a minimum:

(i) Class II gaming systems;

(ii) Accounting/auditing systems;

(iii) Cashless systems;

(iv) Voucher systems;

(v) Player tracking systems; and

(vi) External bonusing systems.

(2) If the computer system cannot deny access after a predetermined number of consecutive unsuccessful attempts to log on, the system must record unsuccessful log on attempts.

(f) Remote access controls.

(1) For computer systems that can be accessed remotely, the written system of internal controls must specifically address remote access

~~**procedures including, at a minimum:**~~

~~**(i) Record the application remotely accessed, authorized user's name and business address and version number, if applicable;**~~

~~**(ii) Require approved secured connection;**~~

~~**(iii) The procedures used in establishing and using passwords to allow authorized users to access the computer system through remote access;**~~

~~**(iv) The agents involved and procedures performed to enable the physical connection to the computer system when the authorized user requires access to the system through remote access; and**~~

~~**(v) The agents involved and procedures performed to ensure the remote access connection is disconnected when the remote access is no longer required.**~~

~~**(2) In the event of remote access, the information technology employees must prepare a complete record of the access to include:**~~

~~**(i) Name or identifier of the employee authorizing access;**~~

~~**(ii) Name or identifier of the authorized user accessing system;**~~

~~**(iii) Date, time, and duration of access; and**~~

~~**(iv) Description of work performed in adequate detail to include the old and new version numbers, if applicable of any software that was modified, and details regarding any other changes made to the system.**~~

Justification: Revision is to clarify and expand on the physical IT Infrastructure access areas and key application systems under the control objective.

(a) *Physical Access and Maintenance Controls* (1) The critical IT systems and equipment for each gaming application (e.g., bingo) and each application for financials, shall be maintained in a physically secured area. The area housing the critical IT systems and equipment for each gaming and other critical IT systems and equipment shall be equipped with the following:

(i) Uninterruptible power supply to reduce the risk of data loss in the event of an interruption to commercial power. Components in a player interface cabinet are not required to maintain an uninterruptible power supply.

(ii) A security mechanism to prevent unauthorized physical access to areas housing critical IT systems and equipment for gaming and financial applications, such as traditional key locks, biometrics, combination door lock, or electronic key card system.

(2) Access to areas housing critical IT systems and equipment for gaming and financial applications, including vendor supported systems, shall be limited to authorized IT personnel as approved by the Tribal gaming regulatory authority. Non-IT personnel, including vendors of the gaming computer equipment, shall only be allowed access to the areas housing critical IT systems and equipment for gaming applications when authorized by IT Management in accordance with IT policies and procedures. At a minimum, such policies and procedures shall require monitoring of personnel during each access.

(i) A record of each access by non-IT personnel shall be maintained by IT management to include the name of the visitor(s), time and date of entry, reason for

visit, company or organization and the name of the designated and authorized personnel escorting the visitor, followed by the time and date of visitor departure.

(ii) The administration of the electronic security systems, if used to secure areas housing critical IT systems and equipment, shall be performed by personnel independent of a gaming or financial department in accordance with policies and procedures approved by the Tribal gaming regulatory authority.

Justification: System Parameters (logical security), is the continuation of Physical Access and Maintenance Controls (physical security) above. Strong end-user password complexity requirements have been defined, per system allowance. System log review, system incidents and system log retention has been further defined.

(b) *System Parameters* (1) The computer systems, including application software, shall be logically secured through the use of passwords, biometrics, or other means approved by the Tribal gaming regulatory authority.

(2) Security parameters for passwords, if configurable, shall meet the following minimum requirements:

(i) Passwords shall be changed at least once every 90 days (quarterly).

(ii) Passwords shall be 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.

(iii) If the system maintains an electronic record of old or previously used passwords, passwords may not be re-used for a period of 18 months.

(iv) User accounts shall be automatically locked out after 3 failed login attempts. The system may, subject to the approval of the TGRA, release a locked out account after 30 minutes has elapsed.

(v) The written system of internal controls shall delineate whether the system is configurable for security parameters for passwords, including temporary passwords, and to what extent the system is configurable in meeting the security parameter requirements.

(3) A system event log (incident log) or series of reports/logs for critical IT systems, if capable of being created by all components that communicate within the gaming network, will be configured to track the following events:

(i) Failed login attempts.

(ii) Changes to live data files occurring outside of normal program and operating system execution.

(iii) Changes to operating system, database, network, and application policies and parameters.

(iv) Audit trail of information changed by administrator accounts; and

(v) Changes to date/time on master time server.

(4) (i) Daily system event logs shall be reviewed at least once weekly (for each day of the entire previous week) by IT personnel other than the system administrator for events listed in 543.16 (b) (3). For Tier A and B gaming operations, the system administrator restriction is not applicable. The system event logs shall be maintained for a minimum of the preceding seven (7) days. Documentation of this review (e.g., log, checklist, notation on reports) shall be maintained for a minimum of ninety (90) days and include the date, time, name of individual performing the review, the exceptions noted, and any follow-up of the noted exception.

(ii) An automated tool that polls the event logs for all gaming and financial related servers, and provides the system administrators notification of the above may be used. Maintaining the notification for ninety (90) days shall serve as evidence of the review.

(5) Exception reports, if capable, for components that communicate within the gaming network (e.g. changes to system parameters, corrections, overrides, voids, etc.) shall be maintained and include at a minimum:"

(i) Date and time of alteration;

(ii) Identification of user that performed alteration;

(iii) Data or parameter altered;

(iv) Data or parameter value prior to alteration; and

(v) Data or parameter value after alteration.

Justification: The selection, provisioning and management of user accounts further defined, as well as system administrator responsibilities within user accounts. Quarterly user access review has been established.

(c) *User Accounts* (1) Management personnel, or persons independent of the department being controlled, shall establish, or review and approve, user accounts to ensure that, at a minimum, assigned application functions match the employee's current job responsibilities, unless otherwise authorized by management personnel, and to ensure adequate segregation of duties.

(2) At a minimum, the review shall ensure that any previously assigned application function access for the employee's user account is changed to inactive (disabled) prior to the employee accessing their new user account for their role or position in a new department.

(3) User access listings shall include, if the system is capable of providing such information, at a minimum:

(i) Employee name and title or position.

(ii) User login name.

(iii) Full list and description of application functions that each group/user account may execute. This list may be available in a separate report if the menu functions are easily referenced between the user access listing report and the menu function report.

(iv) Date and time account created.

(v) Date and time of last login.

(vi) Date of last password change.

(vii) Date and time account disabled/deactivated.

(viii) Group membership of user account, if applicable.

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

(5)The system administrator or designee and the Tribal gaming regulatory authority shall be notified as soon as possible when an employee is known to be no longer employed (e.g., voluntary or involuntary termination of employment). Upon

notification ,the system administrator shall change the status of the employee's user account from active to inactive (disabled) status

(6) The system administrator or designee and the Tribal gaming regulatory authority shall be notified as soon as possible when a user's authorized remote access capability is suspended or revoked. Upon notification, the system administrator or designee shall change the status of the user's account from active to inactive (disabled) status.

(7) User access listings for gaming applications at the application layer shall be reviewed quarterly by personnel independent of the authorization and user provisioning processes. The review shall consist of examining a sample of at least 25 users included in the listing or more as determined by the Tribal gaming regulatory authority. The reviewer shall maintain adequate evidence to support the review process, which shall include 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, the reviewer shall determine whether:

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

(ii) The assigned functions provide an adequate segregation of duties;

(iii) Terminated users' accounts have been changed to inactive (disabled) status;

(iv) Passwords have been changed within the last ninety (90) days. The review for password changes within 90 days applies regardless of whether the system

parameter has been configured to forcefully request a password change every 90 days.

(v) There are no inappropriate assigned functions for group membership, if applicable.

Justification: Revision further defines generic user account configuration, functionality and assignment. Generic user accounts are defined as user accounts that are shared by multiple users (using the same password) to gain access to gaming systems and applications.

(d) ***Generic User Accounts*** **(1) Generic user accounts at the operating system level, if used, shall be configured such that the user is automatically brought to the application logon screen immediately upon logging into the operating system. The generic user accounts must also be configured such that the user is logged out of the operating system automatically upon exiting the application.**

(2) Generic user accounts at the application system level shall be prohibited unless user access is restricted to inquiry or read only functions.

Justification: Service and default accounts utilization defined. Compliance suggestions provided. Default accounts are user accounts with predefined access levels usually created by default at installation for operating systems, databases and applications. Accounts for a particular application system or database may be system generated via query by the Administrator of each system or database.

(e) ***Service and Default Accounts*** **(1) Service accounts, if utilized, shall be configured in a manner that prevents unauthorized and inappropriate usage to gain logical access to an application and the underlying databases and operating system. The individual responsible for the documentation indicating the method used to prevent unauthorized and inappropriate usage of these service accounts shall be identified in the written system of internal controls, that include at a minimum:.**

(i) Service accounts shall be configured such that the account cannot be used to directly log into the console of a server or workstation; and

(ii) Service account passwords shall be changed at least once every 90 days, and deactivated immediately upon the completion of services provided.

(2) User accounts created by default upon installation of any operating system, database or application (default user accounts) shall be configured, which may include deactivation or disabling, to minimize the possibility that these accounts may be utilized to gain unauthorized access to system resources and data. The individual responsible for the documentation indicating the procedures implemented to restrict access through the use of default accounts shall be identified in the written system of internal controls.

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

Justification: System administrative role defined as the individual(s) responsible for maintaining the stable operation of the IT environment to include software, hardware infrastructure and application software.

(f) ***Administrative Access*** **(1) Access to administer the network, operating system, applications, and database security and system parameters shall be limited to supervisory and/or management employees of the IT department or IT employees under the supervision of supervisory and/or management employees of the IT department. If there is no formal IT department, supervisory or management personnel independent of the department using such system and/or application may**

perform the administrative procedures. The Tribal regulatory gaming authority shall be notified by the IT department (or supervisory or management personnel independent of the department using the system, if there is no formal IT department) of those individuals who have been given administrator level access. Such notification shall occur no less than quarterly or whenever changes occur to the listing.

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

(3) An individual independent of the gaming machine department shall daily review the requirements of a system based game and a system supported game ensuring the proper use of split or dual passwords by system administrators. This standard requires a review to confirm that the system requires or warrants the use of split or dual passwords and that split or dual passwords have been used.

(g) *Backups* (1) Daily backup and recovery procedures shall be in place and, if applicable, include:

(1) The IT department shall develop and implement daily backup and recovery procedures which, if applicable, shall address at a minimum the following:

(i) Application data (this standard only applies if data files have been updated).

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

(iii) Database contents and transaction logs.

(2) Upon completion of the backup process, the backup media shall be transferred as soon as practicable to a location separate from the location housing the systems' servers and data being backed up (for temporary and permanent storage). The storage location shall be secured to prevent unauthorized access and provides adequate protection to prevent the permanent loss of any data.

(3) 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 system hardware/software as long as they are secured in a fireproof safe (1000 degrees Fahrenheit for one (1) hour minimum) or in some other manner that will ensure the safety of the files and programs in the event of a fire or other disaster.

(4) Backup system logs, if provided by the system, shall be reviewed by IT personnel or individuals authorized by IT personnel (daily review recommended) at a frequency determined by the Tribal gaming regulatory authority to ensure that backup jobs execute correctly and on schedule. The backup system logs shall be maintained for a time period established by the Tribal gaming regulatory authority.

(5) The IT personnel responsible for the documentation indicating the procedures implemented for the backup processes and for restoring data and application files is delineated in the written system of internal control or policies and procedures .

(i) In support of data restoration procedures, gaming operations shall test data recovery procedures using actual data at least annually, with documentation, review

and IT managerial sign-off of results, which shall be made available to the Tribal gaming regulatory authority upon request.

(h) *Recordkeeping* (1) Critical IT system documentation for all in-use versions of applications, databases, network hardware, and operating systems shall be readily available, including descriptions of hardware and software (including version numbers), operator manuals, etc.

(2) System administrators shall maintain a current list of all enabled generic, system, and default accounts. The documentation shall include, at a minimum, the following:

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

(ii) The user account login name.

(iii) A description of the account's purpose.

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

(3) The current list shall be reviewed by IT management in addition to the system administrator at least once every six months to identify any unauthorized or outdated accounts.

(4) User access listings for all gaming systems shall be retained for at least one (1) day of each month for the most recent five (5) years. The lists may be archived electronically if the listing is written to unalterable media (secured to preclude alteration). If the list of users and user access for any given system is available in electronic format, the list may be analyzed by analytical tools (i.e., spreadsheet or database).

(5) The IT department shall maintain current documentation with respect to the network topology (e.g., flowchart/diagram), deployment of servers housing applications and databases, and inventory of software and hardware deployed (available upon request by authorized internal and external auditors and by Commission personnel). The employee responsible for maintaining the current documentation on the network topology shall be identified in the IT departmental policies and procedures.

(i) ***Electronic Storage of Documentation*** **(1) Documents may be scanned or directly stored to unalterable media (secured to preclude alteration) with the following conditions:**

(i) The storage media shall contain the exact duplicate of the original document.

(ii) All documents stored shall be maintained with a detailed index containing the casino department and date.

(iii) Controls shall exist to ensure the accurate reproduction of records, up to and including the printing of stored documents used for audit purposes.

(j) ***Network Security*** **(1) If guest networks are offered (such as networks that provide internet access for patrons, hotel guests, or vendors), adequate logical segregation, as certified by IT management, shall be provided of the guest network from the network used to serve access to gaming and financial related applications and devices. Traffic on guest networks shall be non-routable to the network serving gaming and financial-related applications and devices.**

(2) Production networks serving gaming systems shall be secured from outside traffic (e.g., firewall and routers) such that systems are configured to detect and report security related events (security logs).

(i) IT personnel responsible for documentation and review of procedures for detecting and reporting security related events shall be identified in the written system of internal control or policies and procedures.

(ii) If the system is configurable, the system shall log:

(A) Unauthorized logins,

(B) Failed login attempts,

(C) Other security related events (incident logs),

(iii) Deactivate all unused physical and logical ports and any in-bound connections originating from outside the network.

(A) Other security related events to be captured by the system include changes to live data files and any other unusual transactions.

(B) [Reserved]

(3) Network shared drives containing application files and data for all gaming and financial related applications shall be secured such that only authorized personnel may gain access.

(4) Server consoles, and unattended user terminals in gaming areas shall be configured to automatically secure themselves after a configurable period of inactivity elapses, the amount of time to be determined by IT department personnel. The time period of inactivity shall be documented in the written system of internal

controls or IT policies and procedures. Users shall supply proper login credentials to regain access to the terminal or console.

(5) Login accounts and passwords required to administer network equipment shall be secured such that only authorized IT personnel may gain access to these devices. The passwords for these accounts shall meet system security parameters in accordance with IT policies and procedures, and shall be immediately disabled when IT personnel are terminated. The Tribal gaming regulatory authority shall be immediately notified of such actions.

(k) *Changes to Production Environment* (1) The individual responsible for the documentation indicating the process for managing changes to the production environment shall be identified in the written system of internal control or IT policies and procedures. Control shall include all changes to the production environment (operating system, network, databases, and applications) that relate to critical IT, gaming and applications systems. This process includes at a minimum:

(i) Proposed changes to the production environment shall be evaluated sufficiently by management personnel prior to implementation;

(ii) Proposed changes shall be properly and sufficiently tested prior to implementation into the production environment;

(iii) A strategy of reverting back to the last implementation shall be used (rollback plan) if the installation is unsuccessful and the rollback plan shall be tested prior to implementation to the production environment; and;

(iv) Sufficient documentation shall be maintained evidencing management approvals, testing procedures and results, rollback plans, and any issues/resolutions encountered during implementation.

(l) *Remote Access* (1) For each critical IT system application that is accessible remotely for purposes of obtaining vendor support, the written system of internal control or policies and procedures, as approved by the Tribal gaming regulatory authority, shall specifically address remote access procedures including, at a minimum:

(i) An automated or manual remote access log that denotes the following:

(A) name of authorized IT technician granting authorization;

(B) vendor's business name and name of authorized programmer;

(C) reason for network access;

(D) critical IT system application to be accessed,

(E) work to be performed on the system and

(F) date, time and approximate duration of the access. Description of work performed shall be adequately detailed to include the old and new version numbers of any software that was modified, and details regarding any other changes made to the system. Final duration of access will be annotated upon termination of the vendors' network connection.

(ii) For computerized casino accounting systems, the approved secured connection shall be such that the system can only be accessed from an authorized authenticated user.

(iii) The method and procedures used in establishing and using unique user IDs, passwords and IP addressing to allow authorized vendor personnel to access the system through remote access.

(iv) IT personnel, by name and role, shall be authorized by IT Management to enable the method of establishing a remote access connection to the system. Such authorizations shall be submitted to the Tribal gaming regulatory authority no less than twice annually.

(v) The name and role of IT personnel involved and procedures performed to ensure the method of establishing remote access connection shall be disabled when vendor remote access is no longer required and not in use. The same shall be submitted to the Tribal gaming regulatory authority no less than twice annually.

(2) User accounts used by vendors shall 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 shall be returned to a disabled state.

(3) If remote access to the production network (live network) is permissible, and allows access to critical IT system applications, such access shall be logged automatically by the device or software where access is established if such logging is capable within system configurations.

(m) ***Information Technology Department*** **(1) If a separate IT department is maintained or if there are in-house developed systems, the IT department shall be independent of all gaming departments (e.g., cage, count rooms, etc.) and operational departments.**

(2) IT personnel shall be precluded from access to wagering instruments and gaming related forms (e.g., player interface jackpot forms). IT personnel shall be restricted from having unauthorized access to cash or other liquid assets as well as initiating general or subsidiary ledger entries.

(n) ***In-house Developed Systems*** **(1) If source code for gaming and/or financial related software is developed or modified internally, a process (systems development life cycle) shall be adopted to manage this in-house development. The individual responsible for the documentation indicating the process in managing the development or modification of source code shall be identified in the written system of internal control or IT policies and procedures. The process shall address, at a minimum:**

(i) Requests for new programs or program changes shall be reviewed by IT supervisory personnel. Approvals to begin work on the program shall be documented.

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

(iii) Sufficiently documenting software development and testing procedures through system development life cycle (SDLC) or other suitable, management approved process. Documentation of approvals, systems development, testing, results of

testing, and implementation into production. Documentation shall include a record of the final program or program changes, including evidence of user acceptance, date in service, programmer, and reason for changes, shall be documented and maintained.

(iv) Physical and logical segregation of the development and testing environment from the production environments.

(v) Adequate segregation of duties (i.e., those who develop/test code do not have access to introduce new or modified code into the production environment). In addition, a system administrator shall be precluded from developing/testing code which will be introduced into the production environment.

(vi) Secured repositories for maintaining code history.

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

(2) All of the in-house developed systems described within this section must be submitted to the TGRA for approval prior to being implemented on the gaming network.

(o) *Purchased Software Programs* (1) For critical IT systems, documentation shall be maintained and include, at a minimum, the date the program was placed into service, the nature of the change (if applicable), a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of the IT technicians who performed such procedures.

(i) Testing of new and modified programs shall be performed (by the gaming operation or the system manufacturer) and documented prior to full implementation, subject to Tribal gaming regulatory approval.

(ii) [Reserved]

(2) [Reserved]