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

(a) General controls for gaming hardware and software.

(1) Management shall take an active role in making sure that physical and logical security measures are implemented, maintained, and adhered to by personnel to prevent unauthorized access that could cause errors or compromise data or processing integrity.

(i) Management shall ensure that all new gaming vendor hardware and software agreements/contracts contain language requiring the vendor to adhere to tribal internal control standards applicable to the goods and services the vendor is providing.

(ii) Physical security measures shall exist over computer, computer terminals, and storage media to prevent unauthorized access and loss of integrity of data and processing.

(iii) Access to systems software and application programs shall be limited to authorized personnel.

(iv) Access to computer data shall be limited to authorized personnel.

(v) Access to computer communications facilities, or the computer system, and information transmissions shall be limited to authorized personnel.

(vi) Standards in paragraph (a) (1) of this section shall apply to each applicable department within the gaming operation.

(2) The main computers (i.e., hardware, software, and data files) for each gaming application (e.g., keno, race and sports, gaming machines, etc.) shall be in a secured area with access restricted to authorized persons, including vendors.

(3) Access to computer operations shall be restricted to authorized personnel to reduce the risk of loss of integrity of data or processing.

(4) Incompatible duties shall be adequately segregated and monitored to prevent error in general information technology procedures to go undetected or fraud to be concealed.

(5) Non-information technology personnel shall be precluded from having unrestricted access to the secured computer areas.

(6) The computer systems, including application software, shall be secured through the use of passwords or other approved means where applicable. Management personnel or persons independent of the department being controlled shall assign and control access to system functions.

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

(i) Each user shall have their own individual password;

(ii) Passwords shall be changed at least quarterly with changes documented; and

(iii) For computer systems that automatically force a password change on a quarterly basis, documentation shall be maintained listing the systems and the date the user was given access.

(8) Adequate backup and recovery procedures shall be in place that include:

(i) Frequent backup of data files;

(ii) Backup of all programs;

(iii) Secured off-site storage of all backup data files and programs, or other adequate protection; and

~~**(iv) Recovery procedures, which are tested on a sample basis at least annually with documentation of results.**~~

~~**(9) Adequate information technology system documentation shall be maintained, including descriptions of hardware and software, operator manuals, etc.**~~

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., keno, pari-mutuel, gaming machines, etc.) 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:**

> **Comment** (December): A definition for "critical IT systems and equipment" needs to be developed.
>
> **Response:** Agree. Definition will be developed.
>
> **Comment** (December): Defining what constitutes "critical IT systems and equipment" should be left to the Tribal gaming regulatory authority to determine.
>
> **Response:** Disagree. What constitutes "critical IT systems and equipment" needs to be clearly defined and not left open.

(i) Redundant power sources to reduce the risk of data loss in the event of an interruption to commercial power. Components in a gaming machine device cabinet are not required to maintain a redundant power source.

> **Comment** (December): A redundant power source will not eliminate the risk of data loss because there will always be a "gap" between the time one source ends and the other one "kicks in". Recommend replacing "redundant power sources" with "uninterruptible power supply".

Response: Agree. Revised accordingly.

Proposed revision as a result of December comments:

(i) Uninterruptible power supply to reduce the risk of data loss in the event of an interruption to commercial power. Components in a gaming machine device 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 restricted to authorized IT personnel. 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 and with periodic monitoring by IT personnel during each access.

Comment (December): Recommend replacing "restricted to authorized IT personnel" with "limited to authorized IT personnel as approved by the Tribal gaming regulatory authority".

Response: Agree. Revised accordingly.

Comment (December): Do not want to preclude access by individuals with legitimate job responsibilities requiring access. Recommend adding "in accordance with IT policies and procedures" following "when authorized by IT Management."

Response: Agree. Revised accordingly.

Comment (December): Periodic monitoring is not sufficient oversight. Recommend deleting "and with periodic monitoring by IT personnel during

each access." And adding "At a minimum such policies and procedures shall require monitoring of personnel during each access."

Response: Agree. Revised accordingly.

Proposed revision as a result of December comments:

(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 and the name of IT personnel authorizing the access, followed by the time and date of visitor departure.

Note: Subsequent to the initial dissemination of the proposed revisions to 542.16, it was recommended that the information in the record of access by non-IT personnel include the company or organization. This was included in the second dissemination of the proposed revisions but was not specifically reviewed during the most recent Committee meeting.

Comment (December): Recommend replacing "the name of IT personnel authorizing the access" with "the name of the designated and authorized personnel escorting the visitor"

Response: Agree. Revised accordingly.

Proposed revision as a result of December comment:

(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.

> **Comment** (December): Recommend adding "in accordance with policies and procedures approved by the Tribal gaming regulatory authority" following "when authorized by IT Management."
>
> **Response:** Agree. Revised accordingly.

Proposed revision as a result of December comment:

(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.

(b) Independence of information technology personnel.

(1) The information technology personnel shall be independent of the gaming areas (e.g., cage, pit, count rooms, etc.). Information technology personnel procedures and controls should be documented and responsibilities communicated.

(2) Information technology personnel shall be precluded from unauthorized access to:

(i) Computers and terminals located in gaming areas;

(ii) Source documents; and

~~**(iii) Live data files (not test data).**~~

~~**(3) Information technology personnel shall be restricted from:**~~

~~**(i) Having unauthorized access to cash or other liquid assets; and**~~

~~**(ii) Initiating general or subsidiary ledger entries.**~~

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:

> **Comment** (December): Recommend removing "if configurable" from (b) (2) and adding "if configurable" to (b) (2) (ii)
>
> **Response:** Disagree. The use of the words "if configurable" is intended to communicate that if the system is not capable of satisfying the requirement, then the requirement is not applicable.
>
> **Comment** (December): Recommendation (above) withdrawn.

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

(ii) Passwords shall be strong passwords of 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.

> **Comment** (December): What does "strong" mean? The word should either be defined or deleted.
>
> **Response:** Agree**.** The criteria following "strong passwords" defines what comprises "strong passwords". Therefore, reference to "strong" can be deleted.

Proposed revision as a result of December comment:

(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) 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.

> **Comment** (December): Recommend adding "If the system maintains an electronic record of old or previously used passwords" at the beginning of the sentence.
>
> **Response:** Agree. Modified accordingly.
>
> **Comment** (December): In order to continue to use the same password, an individual could simply change his/her password ten times in rapid succession. Recommend deleting "or passwords may not be re-used within the last ten password changes."
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comments:

(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 release a locked out account after 30 minutes has elapsed.

> **Comment** (December): Recommend adding "subject to the approval of the Tribal gaming regulatory authority" following "the system may".
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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, and to what extent the system is configurable in meeting the security parameter requirements.

> **Comment** (December): Recommend adding (vi) The IT department shall develop a written policy and procedure that is approved by the TGRA, regarding the issuance of temporary passwords.
>
> **Response:** Agree that temporary passwords should be included in the system of internal controls.

Proposed revision as a result of December comment:

(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 logs) or series of reports/logs for operating systems (including the network layer) and gaming and financial applications, if capable of being generated by the system, s hall be configured to track the following events:

> **Comment** (December): This requirement should only pertain to critical IT systems, not all operating systems. Recommend replacing "operating systems" with "critical IT systems" and deleting "(including the network layer) and gaming and financial applications"
>
> **Response:** Agree. Revised accordingly.
>
> **Comment** (December): Recommend revising as follows: "A system event log (incident log) or series of report/logs, if capable of being created by all components that communicate within the gaming network will be configured to track the following events:"

Response: Agree. Revised accordingly.

Proposed revision as a result of December comments:

(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) 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 542.16 (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 seven (7) days, consisting of the period previously reviewed. Evidence of this review (e.g., log, checklist, notation on reports) shall be maintained for a minimum of ninety (90) days and includes the date, time, name of individual performing the review, the exceptions noted, and any follow-up of the noted exception. An automated tool that polls the event logs for all gaming and financial related servers, and provides the system administrator's notification of the

above may be used. Maintaining the notification for ninety (90) days may serve as evidence of the review.

> **Comment** (December): Recommend breaking this standard down into several standards for readability; a suggestion would categorize the standards according to critical and non-critical systems.
>
> **Response**: Agree to break standard down to facilitate readability. Disagree as to proposed method of categorization as there is no difference in findings between critical and non-critical systems.

Proposed revision as a result of December comment:

(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 MICS (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 seven (7) days, consisting of the period previously reviewed. Evidence of this review (e.g., log, checklist, notation on reports) shall be maintained for a minimum of ninety (90) days and includes the date, time, name of individual performing the review, the exceptions noted, and any follow-up of the noted exception.

> **Note:** On review it was determined that "MICS" should be replaced with "542.16" for consistency in referencing.
>
> **Comment** (December): "Daily system event logs" should be included in the definition section.
>
> **Response:** Agree. Definition will be added to 542.2
>
> **Comment** (December): Recommend adding "the preceding" before "seven" and deleting "consisting of the period previously reviewed."
>
> **Response:** Agree. Revised accordingly.

Comment (December): Recommend replacing "evidence" with "documentation" for consistency with other portions of the MICS.

Response: Agree. Revised accordingly.

Proposed revision as a result of December comments and note:

(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 542.16 (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 of being produced by the system, (e.g., changes to system parameters, corrections, overrides, voids, etc.) for each gaming application and financial related application shall be maintained and include at a minimum:

Comment (December): Recommend the following **"**Exception reports for components that communicate within the gaming network (e.g. changes to system parameters, corrections, overrides, voids, etc.) are maintained and include at a minimum:"

Response: Accepted. Modified accordingly.

Note: "are maintained" is modified to "shall be maintained" for consistency.

Proposed revision as a result of December comments and note:

(5) Exception reports 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:"

Comment (December): Recommend adding "if capable" after exception reports.

Response: Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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.

Comment (December): Recommend adding the words "if applicable" to the beginning of (iii), (iv), (v). This is needed because some systems do not have these specified capabilities.

Response: Disagree. Although not all systems may have these capabilities, the addition of "if capable" in 542.16 (b) (5) covers these situations.

(6) The written system of internal control shall indicate the system's capability of producing an exception report and to what extent this report provides specified information.

Comment (December): Please provide clarification on the meaning and intent of this statement and why it is appearing at the end of this section.

Response: The intent of the standard is to specifically delineate information that should be recorded in writing. However, such information would generally be contained in the IT systems documentation e.g. hardware and software descriptions, operator manuals and therefore can be deleted.

Proposed revision as a result of December comment:

~~**(6) The written system of internal control shall indicate the system's capability of producing an exception report and to what extent this report provides specified information.**~~

~~**(c) Gaming program changes.**~~

~~**(1) Program changes for in-house developed systems should be documented as follows:**~~

~~**(i) Requests for new programs or program changes shall be reviewed by the information technology supervisor. 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 shall include, at a minimum, the date the program is to be placed into service, the nature of the change, a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who is to perform all such procedures;**~~

~~**(iii) Testing of new and modified programs shall be performed and documented prior to implementation; and**~~

~~**(iv) 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.**~~

~~**(2) [Reserved]**~~

Justification: In-house developed software systems and purchased software systems relocated further down in document. 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, will establish, or review and approve, user accounts for new employees. Provisioning for user accounts consist of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties.

> **Comment** (December) Standard reads more like a statement rather than a standard and therefore recommend revising accordingly.
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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) Provisioning of user accounts for employees who transfer to a new department shall be performed, or reviewed and approved, by management personnel, or persons independent of the department being controlled. Any previously assigned

application function access for the employee's user account shall be changed to inactive (disabled) prior to the employee accessing their new user account for their role or position in a new department.

> **Comment** (December) Standard reads more like a statement rather than a standard and therefore recommend revising accordingly.
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

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

> **Comment** (December): With regard to the last sentence of this section (viii), please provide clarification on the meaning and intent of this statement and why it is appearing at the end of this section.
>
> **Response:** Agree to delete. Deleted accordingly.

Proposed revision as a result of December comment:

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

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

(5) The system administrator shall be 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 shall change the status of the employee's user account from active to inactive (disabled) status. The written system of internal control shall delineate the process and reasonable time period in notifying the system administrator for updating the terminated employee's user account and the procedures established in preventing the employee from having unauthorized access to a user terminal.

Comment (December): Recommend adding the TGRA as also being notified at the same time the system administrator is notified; also recommend changing "reasonable time" to "as soon as possible" to be consistent with the subsequent section(s).

Response: Agree. Modified accordingly.

Comment (December): With regard to the last sentence of this section, please provide clarification on the meaning and intent of this statement and why it is appearing at the end of this section.

Response: Agree to delete. Deleted accordingly.

Proposed revision as a result of December comments:

(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) The system administrator shall be 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 shall change the status of an employee's user account with remote access capability from active to inactive (disabled) status. The written system of internal control shall delineate the process in notifying the system

administrator as soon as possible for immediately updating the terminated employee's user account with remote access capability and the procedures established in preventing the employee from having unauthorized remote access.

Comment (December): Recommend adding the TGRA as also being notified at the same time the system administrator is notified; also recommend changing "reasonable time" to "as soon as possible" to be consistent with the subsequent section(s).

Response: Agree. Modified accordingly.

Comment (December): Standard should not only apply to employees, should apply to anyone with a user account with remote access capability.

Response: Agree. Modified accordingly.

Comment (December): With regard to the last sentence of this section, please provide clarification on the meaning and intent of this statement and why it is appearing at the end of this section.

Response: Agree to delete. Deleted accordingly.

Proposed revision as a result of December comment:

(7) 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.

(8) 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 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:

Comment (December): Recommend changing the word "are" to "must be" in the first sentence;

Response: Disagree. In order to maintain consistency in wording "are" has been changed to "shall be".

Comment (December): Does a sample of at least 10% mean that if there are only 50 user access listings that only 5 would need to be reviewed.

Response: Yes**.**

Comment (December): 10% does not seem like enough. Recommend removing 10%.

Response: Agree. Modified accordingly.

Comment (December): Recommend removing "(with a maximum of 25)" to allow for more discretion of the review.

Response: Agree. Modified accordingly.

Comment (December): If this section is referring to the user access listings in section (3), then we recommend moving it up and immediately after that section.

Response: Disagree. (3) is defining the controls relevant to user access listings and (7) is defining the independent auditing procedures.

Proposed revision as a result of December comments:

(8) 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 employee's user accounts have been changed to inactive (disabled) status;

> **Comment** (December): Recommend deleting "employee's" as not all users will be employees.
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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.

~~**(d) Security logs.**~~

~~**(1) If computer security logs are generated by the system, they shall be reviewed by information technology supervisory personnel for evidence of:**~~

~~**(i) Multiple attempts to log-on, or alternatively, the system shall deny user access after three attempts to log-on;**~~

~~**(ii) Unauthorized changes to live data files; and**~~

~~**(iii) Any other unusual transactions.**~~

~~**(2) This paragraph shall not apply to personal computers.**~~

Justification: Security log implementation and review moved further down in document. 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.

~~**(e) Remote dial-up.**~~

~~**(1) If remote dial-up to any associated equipment is allowed for software support, the gaming operation shall maintain an access log that includes:**~~

~~**(i) Name of employee authorizing modem access;**~~

~~**(ii) Name of authorized programmer or manufacturer representative;**~~

~~**(iii) Reason for modem access;**~~

~~**(iv) Description of work performed; and**~~

~~**(v) Date, time, and duration of access.**~~

~~**(2) [Reserved]**~~

Justification: Remote dial-up relocated further down in document. 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 used, shall be 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 Tribal gaming regulatory authority) shall be delineated in the written system of internal control. Suggested methods of compliance include, but are not limited to:**

> **Comment** (December): With regard to the second sentence of this section, please provide clarification on the meaning and intent of this statement.
>
> **Response:** The purpose of the second sentence is to require that the individual (specific position) who is responsible for seeing that this requirement is met, is identified in writing. Sentence will be modified to provide clarity.
>
> **Comment** (December): Recommend deleting "available upon request by Tribal gaming regulatory authority.
>
> **Response:** Agree. Modified accordingly.
>
> **Comment** (December): Recommend changing "suggested methods", which are merely suggestions and not requirements to required minimum components of internal control system.
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comments:

(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 employee 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 immediately upon termination of any system administrators.

> **Comment** (December): I am wondering if the use of the term "system administrator" is appropriate.
>
> **Response:** Agree that "system administrator" may not encompass everything intended. Modified accordingly.

Proposed revision as a result of December comment:

(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 (default 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 employee responsible for the documentation indicating the procedures implemented to restrict access through the use of default accounts shall be delineated in the written system of internal control.

> **Comment** (December): Recommend the following wording **–"**However, the default user accounts may be deactivated or disabled by the system administrator prior to the aforementioned systems or applications being made available to all users on the gaming network."

Response: Agree that standards should include provision for deactivation or disabling of default user accounts. Will modify accordingly.

Comment (December): With regard to the second sentence of this section, please provide clarification on the meaning and intent of this statement.

Response: The purpose of the second sentence is to require that the individual (specific position) who is responsible for seeing that this requirement is met, is identified in writing.

Proposed revision as a result of December comments:

(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 employee 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.

~~**(f) Document storage.**~~

~~**(1) Documents may be scanned or directly stored to an unalterable storage medium under the following conditions.**~~

~~**(i) The storage medium shall contain the exact duplicate of the original document.**~~

~~**(ii) All documents stored on the storage medium shall be maintained with a detailed index containing the gaming operation department and date. This index shall be available upon request by the Commission.**~~

~~**(iii) Upon request and adequate notice by the Commission, hardware (terminal, printer, etc.) shall be made available in order to perform auditing procedures.**~~

~~**(iv) Controls shall exist to ensure the accurate reproduction of records up to and including the printing of stored documents used for auditing purposes.**~~

~~**(v) The storage medium shall be retained for a minimum of five years.**~~

~~**(2) [Reserved]**~~

Justification: The document storage control objective relocated further down in document. 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.**

> **Comment** (December): Recommend adding the following: "The TGRA shall be notified by the IT department of those employees who are given administrator level access, and that such notification shall occur no less than quarterly or whenever changes occur to the listing."
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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 of those employees who have been given administrator level access. Such notification shall occur no less than quarterly or whenever changes occur to the listing.

> **Note:** Upon review it was noted that there is no provision for the situation where there is no formal IT department. Recommend revising as follows:

(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 employees 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.

> **Comment** (December): Please explain what a "split password" and a "dual password" is and the purpose and intent for appearing in this section.
>
> **Response:** A **s**plit password is when two people each possess one portion of a two-segment password. If the password is 8 characters long, one person would have the first 4 characters, the second person the remaining four characters. Dual passwords would require those same two people to input their own full 8 character password in order to open a computer application.

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

> **Comment** (December): Recommend replacing the wording in (1) with the following: The IT department shall develop and implement daily backup and recovery procedures, which if applicable address at a minimum the following:
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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 immediately transferred 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.

> **Comment** (December): Recommend replacing "immediately" with "as soon as practicable".
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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.

(i) This control does not apply to backup data files for computerized keno systems.

(ii) [Reserved]

(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.

> **Comment** (December): Several committee members expressed concern that the standard was too detailed , e.g. the description of what constitutes a fireproof safe and that there should be more left to the discretion of the Tribal gaming regulatory authority.
>
> **Response:** Disagree. It is essential that the back-ups of data files and programs be protected. Based on examples of "secured" files that have been witnessed in the field, specificity is needed.

(4) Backup system logs, if provided by the system, shall be 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 shall be maintained for the most recent 30 days.

> **Comment** (December): Recommend adding language that allows the TGRA to determine the appropriate times periods.
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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 employee(s) responsible for the documentation indicating the procedures implemented for the backup processes and for restoring data and application files shall be delineated in the written system of internal control.

> **Comment** (December): Recommend changing "internal control" to "IT departmental policies and procedures".

Response: Agree to add "or policies and procedures."

Proposed revision as a result of December comment:

(5) The IT employee(s) 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 managerial sign-off of results.

Comment (December): Recommend inserting "IT" before "managerial".

Response: Agree. Modified accordingly.

Comment (December): Recommend adding "which shall be made available to the TGRA upon request" following "results".

Response: The MICS contain an overall statement that makes any and all documents available to the Tribal gaming regulatory authority. Nevertheless, we agree to add the wording requested.. Modified accordingly.

Proposed revision as a result of December comments:

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

Comment (December): Recommend inserting “Critical IT” before “system”.

Response: Agree. Modified accordingly.

Comment (December): Recommend replacing “maintained” with “readily available”

Response: Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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.

Comment (December): Recommend adding “Any exceptions are to be submitted to the TGRA upon completion of the review.” Discussion ensued as to the

purpose of submitting such a document to the TGRA and what the TGRA would do with such a document. Comment withdrawn.

(4) User access listings for all gaming systems shall be to 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 available, the list of users and user access for any given system shall be in electronic format that can be analyzed by analytical tools (i.e., spreadsheet or database) that may be employed by Commission agents.

Comment (December):Recommend rewording standard for clarity.

Response: Agree. Modified accordingly.

Comment (December):Recommend deleting reference to Commission agents.

Response: Agree. Modified accordingly.

Proposed revision as a result of December comments:

(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 delineated in the written system of internal control.

> **Comment** (December): Recommend changing "internal control" to "IT departmental policies and procedures".
>
> **Response:** Agree. Modified accordingly.
>
> **Comment** (December): Recommend replacing "delineated" with "identified".
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comments:

(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. This index shall be available upon Tribal gaming regulatory authority request.

> **Comment** (December): Recommend deleting "This index shall be available upon Tribal Gaming Regulatory Authority request."

Response: Agree. Modified accordingly.

Proposed revision as a result of December comments:

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

(iii) Upon request, hardware (terminal, printer, etc.) shall be provided in order to perform audit procedures.

Comment (December): Recommend deleting "(iii) Upon request, hardware (terminal, printer, etc.) shall be provided in order to perform audit procedures." as unnecessary."

Response: Agree. Modified accordingly.

Proposed revision as a result of December comment (Subsequent item redesignated):

(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 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.**

Comment (December): Recommend adding "as certified by IT management" after "adequate logical segregation" to better define the term.

Response: Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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). IT employees responsible for documentation and review, indicating the procedures for detecting and reporting security related events (available upon request by the Tribal Gaming Authority) shall be delineated in the written system of internal control. A suggested compliance method, if the system allows, is to configure the system to log unauthorized logins, failed login attempts, and other security related events (incident logs); and block all unused ports and any in-bound connections originating from outside the network.

Comment (December): Recommend "segmenting" this section for readability purposes.

Response: Agree. Modified accordingly.

Comment (December): Recommend replacing "block" with "deactivate".

Response: Agree. Modified accordingly.

Comment (December): Recommend clarifying what type of ports this standard applies to.

Response: Agree. "Ports" refers to both physical and logical ports. Modified accordingly.

Comment (December): Recommend changing "internal control" to "IT departmental policies and procedures".

Response: Agree. Will modify for consistency with previous sections.

Proposed revision as a result of December comments:

(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 employees 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 management. The time period of inactivity shall be documented in the gaming operation written system of internal control. Users shall supply proper login credentials to regain access to the terminal or console.

> **Comment** (December): Recommend replacing "management" with "IT department personnel."
>
> **Response:** Agree. Modified accordingly.
>
> **Comment** (December): Recommend adding "IT department policies and procedures."
>
> **Response:** Agree. Will modify for consistency with previous sections.

Proposed revision as a result of December comments:

(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 and shall be immediately disabled when IT personnel are terminated.

> **Comment** (December): Recommend adding: "in accordance with the IT departments written policies and procedures" after "parameters".
>
> **Response:** Agree. Modified accordingly.

Comment (December): Recommend adding "Additionally, the TGRA shall be notified of these changes and terminations as they occur" after "terminated".

Response: Agree to add comparable language. Modified accordingly.

Comment (December): Recommend requiring that notification to TGRA be immediate.

Response: Agree. Modified accordingly.

Proposed revision as a result of December comments:

(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 employee responsible for the documentation indicating the process for managing changes to the production environment (available upon request by the Tribal gaming regulatory authority) shall be delineated in the written system of internal control. Control includes all changes to the production environment (operating system, network, databases, and applications) that relate to critical IT, gaming and applications systems. This process shall include at a minimum:

Comment (December): Recommend deleting "(available upon request by the Tribal Gaming Regulatory Authority)".

Response: Agree. Modified accordingly.

Comment (December): Recommend changing "internal control" to "IT departmental policies and procedures".

Response: Agree. Will modify for consistency.

Note: Upon review, changed "delineated" to "identified" for consistency with prior standards.

Proposed revision as a result of December comments and note:

(1) The employee 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 install is unsuccessful and the rollback plan shall be tested prior to implementation to the production environment and;

Comment (December): Recommend replacing "install" with "installation".

Response: Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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 computerized server-based, server-supported or mobile gaming application that is accessible remotely for purposes of obtaining vendor support, the written system of internal control must specifically address remote access procedures including, at a minimum:**

> **Comment** (December): Recommend replacing "computerized server-based, server-supported or mobile gaming" with "critical IT system".
>
> **Response:** Agree. Modified accordingly.
>
> **Comment** (December): Recommend changing "internal control" to "IT departmental policies and procedures".
>
> **Response:** Agree. Will modify for consistency with previous sections.
>
> **Comment** (December): Recommend adding "as approved by the TGRA" after "policies and procedures"
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comments:

(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:

> **Note:** Upon subsequent review, designation of following items corrected from "numbers" to upper case letters.

(A) name of authorized IT technician granting authorization;

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

(C) reason for network access;

(D) gaming application to be accessed;

> **Comment** (December): Recommend replacing "gaming" with "critical IT system".
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of December comment:

(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 cashless wagering systems (on-line gaming machine metering system), the approved secured connection shall be such that the system can only be accessed from the vendor's place of business.

> **Comment** (December): Recommend replacing "cashless wagering systems (on-line gaming machine metering system)" with "computerized casino accounting systems" for consistency in use of terminology.
>
> **Response:** Agree. Modified accordingly.
>
> **Comment** (December): Discussion ensued relative to feasibility of requiring remote access only from vendor's place of business as well as to how compliance would be audited. Recommendation made to replace "from the vendor's place of business" with "from the vendor's IP address."

Response: Agree. Modified accordingly.

Proposed revision as a result of December comments:

(ii) For computerized casino accounting systems, the approved secured connection shall be such that the system can only be accessed from the vendor's IP address.

Comment (December): Subsequent discussion resulted in the recommendation that "from the vendor's IP address" be replaced with "from an authorized authenticated user."

Response: Agree. Modified accordingly.

Proposed revision as a result of subsequent December comment:

(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, authorized by IT Management to enable the method of establishing a remote access connection to the system.

Comment (December): Recommend adding "shall be" after the word "role".

Response: Agree. Modified accordingly.

Comment (December): Recommend adding to the end of the sentence: "the same to be submitted to the TGRA no less than twice annually."

Response: Agree to add comparable language. Modified accordingly.

Proposed revision as a result of subsequent December comment:

(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.

Comment (December): Preceding item should be numbered (v).

Response: Agree. Modified accordingly.

Comment (December): Recommend adding same trailing verbiage as added to (iv)

Response: Agree. Modified accordingly.

Proposed revision as a result of subsequent December comments:

(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.

(vi) Any additional requirements relating to remote access.

Comment (December): Preceding item should be numbered (vi).

Response: Agree. Modified accordingly.

(vii) Any additional requirements relating to remote access.

Comment (December): Recommend deleting the preceding item due to lack of specificity.

Response: Agree. Deleted accordingly.

Proposed revision as a result of subsequent December comment:

~~**(vii) Any additional requirements relating to remote access.**~~

(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) Remote access for all vendors shall be enabled only when approved by authorized IT personnel.

> **Comment** (December): Recommend replacing "by authorized IT personnel" with "when approved by the TGRA and authorized by the authorized IT personnel."
>
> **Response:** Disagree. Approval/authorization requirements for enabling remote access exist elsewhere in the MICS.
>
> **Comment** (December): Recommend deleting (3) as redundant to other standards.
>
> **Response:** Agree. Deleted accordingly. (Subsequent items renumbered.)

(3) If remote access to the production network (live network) is permissible, and allows access to gaming related applications, such access shall be logged automatically by the device or software where access is established.

> **Comment** (December): Recommend adding "If applicable" to the beginning of the sentence because some gaming operations only have VPN access that is turned on and off and no information is logged. As this standard currently reads, the NIGC is assuming that the gaming operation or the IT department has a network utility capable of meeting this standard.
>
> **Response:** Agree with issue raised. Will modify with comparable wording.

Proposed revision as a result of subsequent December comment:

(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, pit, count rooms, etc.) and operational departments.**

(2) IT personnel shall be precluded from access to wagering instruments and gaming related forms (e.g., gaming machine jackpot forms, table games fill/credit forms, etc.). 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 employee responsible for the documentation indicating the process in managing the development or modification of source code (available upon request to the Tribal gaming regulatory authority) shall be delineated in the written system of internal control. The process must address, at a minimum:**

> **Comment** (December): Recommend deleting '(available upon request to the Tribal Gaming Regulatory Authority" since all documents are available to the TGRA.
>
> **Response:** Agree. Modified accordingly.
>
> **Comment** (December): Recommend replacing "delineated" with identified.
>
> **Response:** Agree. Modified accordingly.
>
> **Comment** (December): Recommend modifying reference to "system of internal control" to be consistent with preceding sections.

Response: Agree. Modified accordingly.

Proposed revision as a result of subsequent December comments:

(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 employee 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 who is to perform all such procedures.

Comment (December): Recommend replacing "who" with "which operational department"

Response: Agree. Modified accordingly.

Proposed revision as a result of subsequent December comment:

(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).

> **Comment** (December): Recommend adding (2) as follows "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."
>
> **Response:** Agree. Modified accordingly.

Proposed revision as a result of subsequent December comment:

(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) Documentation shall be maintained and shall 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.

> **Comment** (December): Recommend adding a number 2 which limits the applicability of this section to only that software that is critical to the operation or functionality of the gaming network.
>
> **Response:** Agree with issue raised. Disagree with proposed wording. For consistency with the section, will add "For critical IT systems".

Proposed revision as a result of subsequent December comment:

(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.

> **Comment** (December): Recommend adding "at the discretion of the TGRA" the end of the sentence.

Response: Agree. Modified with comparable wording.

Proposed revision as a result of subsequent December comment:

(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]