21.1 General Information Technology (IT) Standards

A. The IT department shall adhere to all standards located throughout this document, which may or may not be referenced in this Section. Standards in this section shall apply to each applicable department within the casino operation.

B. All critical IT systems, storage media (software), data, programs, and equipment (collectively "Critical IT Systems") shall adhere to the standards required in this Section. Critical IT systems include all gaming and/or gaming related systems, but may not be limited to, financial and accounting systems, casino management systems, surveillance systems, key and access control systems and/or related system interfaces.

C. The IT department shall be adequately segregated and independent of all gaming, finance, and operational departments. IT personnel procedures and controls should be documented and responsibilities communicated.

D. IT personnel shall be precluded from unauthorized access to:

1. Computers and terminals located in gaming areas, source documents, and live data files (not test data).

2. Access to or signatory authority over financial instruments and gaming related forms (e.g., gaming machine jackpot forms, table games fill/credit forms, cashless ticket paper, etc.).

3. Having unauthorized Access to cash or other liquid assets as well as initiating general or subsidiary ledger entries.

E. Any vendor utilized for the purchase or lease of hardware and/or software or to provide service and/or maintenance to critical IT systems at any licensed gaming facility must have complied with applicable Cherokee Nation Gaming Commission (CNGC) vendor licensing requirements prior to the sale or lease of hardware or software and/or prior to gaining any access to any critical IT systems.

F. Management shall ensure that all agreement/contracts entered into provide and/or service critical IT systems shall contain language requiring the vendor to comply with the standards in this Section as applicable to the goods and services the vendor is providing. All agreements /contracts verbal or written shall be submitted and placed on file with the CNGC.

G. The operation shall establish and implement IT policies and procedures, as approved by the CNGC, which shall include the

controls established in this Section and throughout this document (as applicable).

H. Controls must identify supervisory personnel independent of the gaming department responsible for ensuring that the department or area is operating in accordance with established policies and procedures.

21.2 Physical Access and Maintenance Controls

A. The critical information technology (IT) systems, software, and equipment shall be maintained in a highly restricted area and physically secured from unauthorized access.

B. The area housing the critical IT systems and equipment shall be equipped with the following:

1. Uninterruptible power supply to reduce the risk of data loss in the event of an interruption to commercial power; and,

2. A security mechanism to prevent unauthorized physical access to areas housing critical IT systems and equipment such as traditional key locks, biometrics, combination door lock, or electronic key card system.

C. Access to areas that house critical IT systems are considered highly restricted and access shall be controlled in accordance with IT policies and procedures, as approved by the CNGC, which shall include the following provisions:

1. Unescorted access to areas housing critical IT systems and equipment, including vendor supported systems, shall be limited to authorized licensed IT personnel of the casino who require access as part of their normal job duties;

2. Licensed non-IT personnel, including vendors shall only be allowed access to the areas housing critical IT systems and equipment when escorted by authorized IT management or IT personnel designated by IT management; and,

3. Any person not licensed by the CNGC must be escorted by authorized licensed IT personnel or have specific approval from the CNGC before entering any area housing critical IT systems and equipment.

D. Licensed IT personnel authorized to enter the areas housing critical IT systems and equipment without escort shall be listed by title. The IT Department is responsible to update the list and provide the list to the CNGC every thirty (30) days. The monthly report shall consist of no less than the title of

authorized persons and a statement indicating any changes or no changes from the previous report which was submitted to the CNGC.

1. The IT departmental policies and procedures shall include provisions for ensuring that only authorized personnel are provided access.

2. For access controlled by a computerized system the access control administrator shall assign and control user access into areas that house critical IT systems and equipment to ensure access is restricted to authorized employees only.

E. All personnel that require an escort to access areas housing critical IT systems and equipment shall record each access on a log to be maintained by IT management or departments designated by IT management and shall include the following:

1. The area being accessed;

2. Name of employee or visitor and company or organization;

3. Date and time of entry;

4. Purpose of visit;

5. Signature and employee number of escort; and,

6. Time of employee/visitor departure.

F. The operation, as approved by the CNGC, shall establish procedures for reviewing access and reporting unauthorized access. Personnel independent of the IT department and access control shall review, at least quarterly, a sample of users that are assigned access to the areas housing critical IT systems and equipment for proper authorization and assurance.

G. All noted unauthorized access shall be investigated with the results documented and submitted to the CNGC.

21.3 Systems Acquisitions and Development

A. Notice must be provided to the CNGC prior to the acquisition and development of any critical IT system as defined under section 21.1 (B) prior to implementation.

B. For in-house developed systems, if source code for financial and/or gaming related software is developed or modified internally, a process (systems development life cycle (SDLC)) shall be adopted to manage this in-house development. The employee responsible for the documentation indicating the process for 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:

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

2. A written plan of implementation for new and modified programs shall be maintained and include, at a minimum;

    a. The date the program is to be placed into service;

    b. The nature of the change (if applicable);

    c. A description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.);

    d. An indication of which operational department is to perform all such procedures; and,

3. Sufficient documentation of the following:

    a. Software development and testing procedures through SDLC or other suitable, management approved process;

    b. Approvals, systems development, testing, results of testing, and implementation into production;

    c. A maintained record of the final program or program changes, including evidence of user acceptance, date in service, programmer, and reason for changes;

    d. Physical and logical segregation of the development and testing environment from the production environments;

    e. 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, the system administrator shall be precluded from developing /testing code that will be introduced into the production environment;

    f. Secured repositories for maintaining code history; and,

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

4. The CNGC may require certain in-house developed programs, or any modifications or upgrades made thereto, to be tested and/or verified by an independent testing laboratory prior to approval.

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

C. Purchased Software Programs

1. For critical IT systems, documentation shall be maintained and include, at a minimum:

a. The date the program was placed into service;

b. The nature of the change (if applicable);

c. A description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.); and,

d. An indication of the IT technicians who performed such procedures.

2. Testing of new and modified programs shall be performed (by the casino operation or the system manufacturer) and documented prior to full implementation, subject to CNGC approval.

D. Software Downloads/Verification

1. Downloads, either automatic or manual, must be performed in accordance with 25 CFR 547.12.

2. Following downloads of any gaming system software; the gaming system must verify the downloaded software using a software signature verification method. Using any method it deems appropriate, the CNGC must confirm the verification.

21.4 Changes to Production Environment

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:

A. Proposed changes to the production environment shall be evaluated sufficiently by management personnel prior to implementation;

B. Proposed changes shall be properly and sufficiently tested prior to implementation into the production environment;

C. 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;

D. End-user testing may be required to assess the effective implementation of the change; and,

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

21.5 System Parameters

A. The computer systems, including application software, shall be logically secured through the use of access credentials, such as passwords, biometrics, or other means approved by the CNGC.

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

1. Each user must have their own unique individual access credential.

2. Passwords shall be changed at least once every ninety (90) days (quarterly);

3. Passwords shall be at least eight (8) characters in length and contain a combination of at least two (2) of the following criteria: upper case letters, lower case letters, numeric and/or special characters;

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

5. User accounts shall be automatically locked out after three (3) failed login attempts. The system may, subject to the approval of the CNGC, release a locked out account after thirty (30) minutes has elapsed; and,

6. 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.

7. For 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.

C. 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:

1. Failed login attempts;

2. Changes to live data files occurring outside of normal program and operating system execution;

3. Changes to operating system database, network, and application policies and parameters;

4. Audit trail of information changed by administrator accounts; and,

5. Changes to date/time on master time server.

D. Logs:

1. 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 21.4 (C). For Tier A and B casino operations, the system administrator restriction is not applicable.

2. 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.

3. Alternatively, an automated tool that polls the event logs for all gaming, casino management, and financial related servers, and provides the system administrators notification of the above, may be used. Notification shall be maintained for ninety (90) days and shall serve as evidence of the review.

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

1. Date and time of alteration;

2. Identification of user that performed alteration;

3. Data or parameter altered;

4. Data or parameter value prior to alteration; and,

5. Data or parameter value after alteration.

21.6 Account Administration

A. 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 the following information as it is available from each system:

   a. Employee name and title or position;

   b. User login name;

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

   d. Date and time account created;

   e. Date and time of last login;

   f. Date of last password change;

   g. Date and time account disabled/deactivated; and,

   h. Group membership of user account, if applicable.

4. When multiple user accounts for one (1) employee per application are used, only one (1) 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 (1) or more Tribal Internal Control Standards (TICS). Additionally, the user account has a unique prefix/suffix to easily identify the users with multiple user accounts within one (1) application.

5. The system administrator or designee and the CNGC shall be notified by the employee's supervisor/manager 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 by the end of the next business day.

6. The system administrator or designee and the CNGC shall be notified by the employee's supervisor/manager 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 by the end of the next business day.

7. Lost or compromised access credentials must be deactivated, secured, or destroyed by the end of the next business day.

8. Only authorized personnel may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts.

9. User access listings for critical IT 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 twenty-five (25) users included in the listing, or more as determined by the CNGC. 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 signature and dates indicating when the user access listing was reviewed. For each of the randomly selected users, the reviewer shall determine whether:

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

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

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

   d. Passwords have been changed within the last ninety (90) days. The review for password

changes within ninety (90) days applies regardless of whether the system parameter has been configured to forcefully request a password change every ninety (90) days; and,

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

B. 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.

C. 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 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:

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

b. Service account passwords shall be changed at least once every one-hundred-eighty (180) days, provided the passwords are alpha-numeric and a minimum of fifteen (15) characters, and deactivated immediately upon the completion of services provided. Otherwise, passwords shall be changed at least once every ninety (90) days.

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 ninety (90) days.

D. Administrative Access

1. Access to administer the network, operating system, applications, and database security and system parameters, shall be limited to employees of the IT department or employees independent of the system operation. Any critical IT system administered by a department other than the IT department, the department must be approved by the CNGC and must show adequate segregation and independence from the operations performed by the system users.

2. Systems being administered shall be enabled to log usage of all administrative accounts. Such logs shall be maintained for thirty (30) days and include the following:

a. Time and date;

b. Login account name;

c. Description of event;

d. The values before the change; and,

e. The value after the change.

21.7 Backups

The IT department shall develop and implement daily backup and recovery procedures

A. Controls must include adequate backup, including, but not limited to, the following:

1. Daily data backup of critical IT systems;

2. Data backup of critical programs or the ability to reinstall the exact programs as needed;

3. Mirrored or redundant data source; and,

4. Redundant and/or backup hardware.

B. Controls must include recovery procedures, including, but not limited to, the following:

1. Data backup restoration;

2. Program restoration; and,

3. Redundant or backup hardware restoration.

C. 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), as approved by CNGC. The storage location shall be secured to prevent unauthorized access and provides adequate protection to prevent the permanent loss of any data.

D. Backup data files and programs can be maintained on site or in another location provided that they are secured in a fireproof safe (one thousand (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.

E. 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 CNGC to ensure that backup jobs execute correctly and on schedule. The backup system logs shall be maintained for a time period established by the CNGC.

F. 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.

1. In support of data restoration procedures, casino operations shall test data recovery procedures using actual data at least annually, with documentation, review and IT managerial sign-off of results.

2. Backup data files and recovery components must be managed with at least the same level of security and access controls as the system for which they are designed to support.

3. Results in section 21.7 (E) (1) shall be made available to the CNGC upon request.

21.8 Record Keeping and Retention

A. Record Keeping

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:

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

    b. The user account login name;

    c. A description of the account purpose; and,

    d. 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 and the system administrator at least once every six (6) 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 CNGC). The employee responsible for maintaining the current documentation on the network topology shall be identified in the IT departmental policies and procedures.

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

    1. The storage media shall contain the exact duplicate of the original document;

    2. All documents stored shall be maintained with a detailed index containing the casino department and date; and,

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

    4. Controls shall exist to ensure the accurate reproduction of records, up to and including the

printing of stored documents used for audit purposes.

5. The storage medium shall be retained for a minimum of five (5) years.

21.9 Network Security

A. 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 and approved by CNGC, shall be provided. The guest network shall not allow 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.

B. Production networks serving gaming and/or gaming related 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).

1. 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.

2. The system shall be capable of logging the following:

a. Unauthorized logins;

b. Failed login attempts; and,

c. Other security related events (incident logs).

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

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

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

D. Server consoles, and unattended user terminals in gaming areas shall be configured to automatically secure themselves after a configurable period of inactivity elapses, as 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.

E. 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 CNGC shall be immediately notified of such actions.

F. Procedures must be established and implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with critical IT systems. All security incidents must be formally documented and responded to within twenty-four (24) hours, unless otherwise provided for by the CNGC.

21.10 Remote Access

A. For each critical IT system application that is accessible remotely, the written system of internal controls or policies and procedures and methods, as approved by the CNGC, shall address remote access procedures that shall include the controls outlined by this section.

B. Vendor Access

1. 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. Verification of the programmer's authorization;

   d. Reason for remote access;

   e. Critical IT system application to be accessed;

   f. Work to be performed on the system; and,

   g. 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 vendor's network connection.

2. For computerized casino accounting systems, the approved secured connection

shall be such that the system can only be accessed from an authorized authenticated user.

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

4. IT personnel, by name and role, shall be authorized by IT Management to enable and/or disable a remote access connection to the system. Such authorizations shall be submitted to the CNGC no less than twice annually.

C. 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.

D. 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.

E. VPN Access/Review Logs

1. Remote access may be granted on a limited basis to active employees whose job duties require access off site with adequate justification documented. Documentation shall be accessible for audit purposes.

2. A list of employees by job title who require remote access shall be updated quarterly and approved by the CNGC. Exceptions to this list shall have adequate justification documented.

3. Internal controls for password/ personal identification number (PIN) integrity in Section 15.12 shall apply to remote access. Computer systems utilizing a remote access connection shall be locked when unattended.

4. Remote access shall be immediately disabled for terminated or suspended employees. In the event of employee transfers, remote access shall remain active only if the employees new job title requires it or if adequate justification is documented.

5. Remote user access logs shall be reviewed quarterly by IT to determine accuracy. Exceptions shall be noted and require evidence of adequate justification to remain active; remote access for all other

exceptions shall be terminated. Evidence of review and approval of all exceptions shall be documented and made accessible for audit purposes.