

SECTION 17  
COMPLIMENTARIES

---

---

**17.1 Standards for Complimentary Services/Items**

A. Each casino operation shall establish and comply with procedures for the authorization, issuance, tracking, and redemption of complimentary services and items, including cash and non-cash gifts, which follow the standards set forth in this Section.

B. The procedures must be approved by the Cherokee Nation Gaming Commission (CNGC) and shall include, but shall not be limited to:

1. The procedures by which the casino operation delegates to its employees the authority to approve the issuance of complimentary services and items;
2. The procedures by which conditions or limits, if any, which may apply to such authority are established and modified (including limits based on relationships between the authorizer and recipient); and,
3. Shall further include effective provisions for audit purposes.

C. Each casino operation shall establish and maintain a complimentary matrix, subject to the approval of the CNGC, which details the specific job titles to which they apply.

D. The complimentary matrix shall at a minimum address:

1. All complimentary types that may be issued by any employee;
2. Authorization limits by each revenue center per customer, per day, (or other defined period);
3. Management compliments (limits issued to unidentified customers); and,
4. Any subsequent changes must be approved by CNGC.

E. Complimentary services and items shall include, but are not limited to, travel, lodging, food, beverages, or entertainment expenses provided directly to the customers and their guests by the casino operation or indirectly to customers and their guests on behalf of the operation by a third party.

F. Complimentary cash gifts shall include, but are not limited to:

1. Public relations payments made for the purpose of resolving complaints by or disputes with casino customers (appeasement payments);
2. Travel or “walk money” payments made for the purpose of enabling a customer to return home.

SECTION 17  
COMPLIMENTARIES

---

---

G. At least monthly, accounting, information technology, or audit personnel that cannot grant or receive complimentary privileges shall prepare reports documenting and recording authorization, issuance, and redemption that include the following information for complimentary services or items for all cash and non-cash gifts, which shall include the following:

1. Name of customer who received the complimentary service or item;
2. Name(s) of authorized issuer(s) of the complimentary service or item;
3. The actual cash value of the complimentary service or item;
  - a. A complimentary service or item provided directly to a customer in the normal course of a casino operation's business shall be recorded at the full retail price normally charged for such service or item by the operation.
  - b. A complimentary service or item not offered for sale to customers in the normal course of a casino operation's business, but provided directly by the operation, shall be recorded at the actual cost to the operation.

c. A complimentary service or item provided directly or indirectly to a customer on behalf of a casino operation by a third party who is affiliated with the operation shall be recorded as if the affiliated third party were the operation.

d. A complimentary service or item provided directly or indirectly to a customer on behalf of a casino operation by a third party who is not affiliated with the casino operation shall be recorded at the actual cost to the operation of having the third party provide such service or item.

4. The revenue center, third party, and/or venue providing the complimentary;
5. The type of complimentary service or item (i.e., cash, food, beverage, etc.); and,
6. Date the complimentary service or item was issued and redeemed.

H. The internal audit or accounting departments shall review the reports required in Part G of this Section at least monthly. The records must be summarized and reviewed for proper authorization and compliance with established authorization thresholds. These detailed reports shall be forwarded to management for review,

SECTION 17  
COMPLIMENTARIES

---

---

submitted to the CNGC and made available, upon request, to the Tribe (Tribal Officials), the NIGC, the Audit Committee, or other authorized entities.

- I. For any computer applications utilized, alternate documentation and/or procedures that provide at least the level of control described by the standards in this section, as approved by the CNGC will be acceptable.

**17.2 Redemption Procedures**

The procedures for redeeming complimentary services/items, shall comply with the standards as set forth in Section 12 – Casino Instruments and Exchanges and Section 4 General Provisions – Currency Handling, as applicable.

SECTION 18  
PLAYER TRACKING SYSTEM

---

---

**18.1 Standards for Player Tracking System**

- A. Each casino operation shall establish and comply with procedures for the authorization, issuance, tracking, and redemption of points awarded through the use of a player tracking system, which shall include the standards set forth in this section.
- B. The system used to track player activity and all related procedures must be approved by the Cherokee Nation Gaming Commission (CNGC), and shall include, but not be limited to:
1. The procedures by which the casino operation delegates to its employees the authority to redeem player tracking points for cash, services, and/or merchandise.
  2. The procedures by which conditions or limits, if any, which may apply to such authority are established and modified; and
  3. Shall further include effective provisions for audit purposes.
- C. Each casino operation shall establish and maintain a permissions matrix, subject to the approval of the CNGC, which details the limits, and/or conditions which may be placed on the authority of its employees to redeem, adjust, or otherwise access player accounts, and the specific job titles to which they apply.
- D. The player tracking system shall be secured so as to prevent unauthorized access (e.g., changing passwords at least every forty-five (45) days and physical access to computer hardware, etc.).
- E. Changes to the player tracking system parameters, such as point structures and employee access, shall be performed by supervisory personnel independent of the player tracking and gaming machine department initiating the change.
- F. Changes to the promotion and external bonusing system parameters, such as the awarding of bonuses, issuance of cashable credits, non-cashable credits, coupons, and vouchers, must be performed by supervisory personnel independent of the department initiating the change. Alternatively, the changes may be made by the department initiating the change if sufficient documentation is generated and the propriety of the changes are verified by supervisory personnel independent of the department initiating the change.
- G. For all changes referenced in paragraph E and F, sufficient documentation must be generated and randomly verified by supervisory personnel independent of the player tracking and gaming machine department on a monthly basis.
- H. All other changes to the player tracking system shall be

SECTION 18  
PLAYER TRACKING SYSTEM

---

---

appropriately documented and submitted to the CNGC.

Financial Transactions shall apply.

**18.2 Player Accounts**

A. Terms and conditions for players club membership must be submitted and approved by the CNGC.

C. For player accounts that provide for customer access, bonusing, and/or self-redemption, account access shall be protected by use of a Personal Identification Number (PIN), as applicable.

B. Customer account generation standards:

1. A computer file for each customer shall be prepared by an employee, with no incompatible functions, prior to the customer being issued an account.

1. The customer shall select his/her PIN to be used in conjunction with the player account access card (i.e. players club membership card).

2. For each account, the system shall require a unique player identification.

2. After entering three (3) sequential incorrect PIN entries, the customer must be directed to the appropriate station to obtain a new PIN by providing proper identification.

3. For each customer file, an employee shall, at a minimum:

3. If the customer forgets, misplaces, or requests a change to their PIN, the same standard shall apply.

a. Record the customer's name, current address, and date of birth

b. At the time the account opened or a change is made to the player's account, the identity of the customer shall be verified by examination of a valid driver's license or other reliable identity credential.

D. The addition or deletion of points to member's accounts other than through normal gaming transactions shall be sufficiently documented (including substantiation of reason for the adjustment) and shall be authorized by supervisory personnel independent of player tracking and gaming machine departments.

c. Where player tracking records are utilized for Financial Transaction reporting, Section 19 –

E. Adjustments to points, as referenced in paragraph D, shall be randomly verified by the accounting / revenue audit department on a monthly basis.

SECTION 18  
PLAYER TRACKING SYSTEM

---

---

- F. For expired points, sufficient documentation shall be generated to ensure that all expired points have been deleted from the player tracking system.
- G. The transfer of player earned points from one (1) account to another account shall be strictly prohibited.
- H. Merging points from multiple accounts belonging to the same customer shall be adequately documented.
- I. No more than three (3) account cards may be active at any time.
- J. Terms and conditions for eligibility to obtain a players club account must be displayed for public view or available upon request.

**18.3 Redemption Procedures**

- A. When redeeming player points, cashiers shall follow the standards in Section 12 – Casino Instruments & Exchanges and Section 4 General Provisions – Currency Handling of this document.
- B. In addition to the redemption standards referenced above, the following standards shall apply:
  - 1. For qualification points, sufficient documentation shall be generated to indicate that all participants are eligible for qualifying games/prizes.

- 2. Employees who redeem points for members are precluded access to lost player account cards, except where there are provisions for immediate deposit into a secured container for retrieval by independent personnel.
- 3. Lost player account cards shall be destroyed within a period not to exceed seven (7) days.

**18.4 Accounting/Auditing Procedures**

- A. The accounting department shall establish procedures subject to approval by the CNGC which adequately account for and audit player tracking programs.
- B. At least monthly, accounting /revenue audit personnel shall review player activity reports for propriety.



SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

purchased with large amounts of currency. Just in case the currency has been “marked” by the federal government during preplanned “sting” operations, the drug dealers want to get rid of (e.g. launder) this currency for new, “clean” currency that is not marked. Banks and casinos are generally used by drug dealers to “wash” or “launder” their monies from the drug transactions. Also, utilizing a bank or a casino sometimes works to provide a “legitimate” look to the transactions.

**Multiple Transaction Log (MTL)** – for purposes of Title 31 currency transaction recordkeeping and reporting requirements, the casino shall maintain a log of all manual currency transactions in the amount of Three Thousand Dollars (\$3,000.00) or more.

**Negotiable Instruments Log (NIL)** – for purposes of the Title 31 currency transaction record keeping requirements, the casino shall maintain a log of all negotiable instruments in the amount of Three Thousand Dollars (\$3,000.00) or more which shall include all checks and drafts (including personal, business, bank, cashier’s, third-party checks, and casino checks), money orders and traveler’s checks, whether or not they are in bearer form or complete.

**Organization** – person other than an individual.

**Person** – an individual, corporation, partnership, trust or estate, joint stock company, association, syndicate, joint venture, or other unincorporated organization or group, and all entities treated as legal personalities.

**Structuring** – For purpose of Title 31 reporting, a person structures a transaction if

that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency, in any amount, at one (1) or more locations where currency transactions are conducted, on one (1) or more days, in any manner, for the purpose of evading the reporting requirements under Title 31. “In any manner” includes, but is not limited to, the breaking down of a single sum of currency exceeding Ten Thousand Dollars (\$10,000.00) into smaller sums, including sums at or below Ten Thousand Dollars (\$10,000.00), including any series of transactions. The transaction or transactions need not exceed the Ten Thousand Dollars (\$10,000.00) reporting threshold at any single casino location on any single day in order to constitute structuring.

**Transaction in Currency** – a transaction involving the physical transfer of currency from one (1) person to another.

### 19.2 General

- A. In accordance with Title 26 – Internal Revenue Code, the casino operation shall establish and comply with procedures for the correct reporting and withholding of certain gaming winnings and/or promotional prizes and awards. These procedures shall be approved by the Cherokee Nation Gaming Commission (CNGC).
- B. Pursuant to the Title 31/Bank Secrecy Act, the casino operation shall develop and implement a Compliance Program and system of internal controls, which includes detailed procedures used to comply with these standards. The

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

Compliance Program shall be approved by the CNGC.

- C. According to Federal Law, the Title 31/Bank Secrecy Act requires the reporting of certain financial transactions and the reporting of suspicious transactions. Additionally, certain records are required to be prepared and maintained relative to Title 31/Bank Secrecy Act for casinos having gross annual gaming revenues in excess of One Million Dollars (\$1,000,000.00).
- D. The purpose of these internal controls is to provide the casino with a framework for developing a system of internal controls/procedures to meet the requirements of Title 26 and Title 31 of the U.S.C.
- E. For any Tribal authorized computer applications, alternate documentation and/or procedures which provide at least the level of control described by these standards will be acceptable, as approved by the CNGC.
- F. Within this document the Title 31/Bank Secrecy Act will be referred to as Title 31.
- G. For purpose of satisfying certain standards in this section, a military / military dependent identification card shall not be copied but may be used to establish a person's identity; however, another form of primary identification must be obtained and copied in order to complete the transaction.

**19.3 Procedures for Reporting Winnings**

- A. Prior to payment of winnings, employees shall determine if winnings are subject to Internal Revenue Service (IRS) reporting requirements. No winnings shall be paid until the appropriate forms (as applicable) have been completed.
- B. IRS Forms – W-2G, 5754, 1099, and 1042-S or other forms designated by the IRS for reporting winnings and/or promotional prizes and awards within this Section shall be referenced as IRS forms for reporting winnings.
- C. IRS Forms for reporting winnings shall be available to all departments that may encounter reportable transactions.
- D. IRS Forms for reporting winnings shall be completed in accordance with, and contain the information required in Title 26 and this document for all reportable winnings and/or promotional prizes and awards.
- E. Before concluding (i.e., prior to payment of winnings) any transaction subject to IRS reporting requirements, the handler of the transaction shall:
  - 1. Obtain and examine two (2) forms of appropriate identification; obtain a copy of the primary form of identification which shall be an official photo identification; if tax identification (Social Security Card) is not available

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

- the winner must complete form W-9 Request for Taxpayer Identification Number and Certification.
2. Acceptable forms of primary identification include a driver's license, military or military dependent identification card, passport, alien registration card, state issued identification card, cedular card (foreign), or other photo identification and/or combination of unexpired documents that contain an individual's name and address and are normally accepted by financial institutions as a means of identification when cashing checks for persons other than established customers.
  3. As an option to requesting the necessary identification and other data from an established customer, information on file may be used if:
    - a. The handler of the transaction knows the customer;
    - b. The customer's name and appropriate identification credentials were obtained from the customer for a previous transaction;
    - c. The information is on file to properly complete the IRS Form; and,
    - d. The customer information on file is periodically updated as follows:
      - i. Copy of original identification credentials;
      - ii. If the customer's Social Security Card was not available to verify identification, the customer must have a completed form W-9 Request for Taxpayer Identification Number and Certification on file;
      - iii. Documentation of the examinations is included in the information on file;
      - iv. Expiration dates of identification credentials are included in the information on file; and,
      - v. The transaction date is prior to the expiration date on file.
  4. The appropriate IRS Form for reporting winnings shall be completed according to the Form instructions and forwarded to the accounting department for review and transmittal to the IRS.

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

**19.4 Title 31 Compliance Program**

- A. In accordance with Part 19.2 (B) of this Section, each Compliance Program shall, at a minimum, provide for:
1. A system of internal controls to assure ongoing compliance;
  2. Internal and/or external independent testing for compliance. The scope and frequency of the testing shall be commensurate with the money laundering and terrorist financing risks posed by the products and services provided by the casino;
  3. Training of casino personnel, including training in the identification of unusual or suspicious transactions, to the extent that the reporting of such transactions is required by Title 31, by other applicable law or regulation, or by the casino's own administrative and compliance policies;
  4. Designated individual and/or department to assure day-to-day compliance; and,
  5. Procedures for using all available information to determine:
    - a. When required to be reported, the name, address, social security number (SSN), and other information, and verification of the same, of a person;
    - b. The occurrence of any transactions or patterns of transactions required to be reported;
    - c. Whether a record required by Title 31 must be made and retained; and,
    - d. For casinos that have automated data processing systems, the use of automated programs to aid in assuring compliance.
- B. Casino management shall review the Title 31 Compliance Program at least annually, and shall consider the following, at a minimum, in determining whether to revise the program:
1. Results of independent testing, including internal or external reviews or audits;
  2. Results of examinations by IRS or other governmental authorities;
  3. Significant changes in operations;
  4. Significant changes in the types of financial services offered;
  5. Implementation of any automated systems and programs that may affect compliance;
  6. Changes/amendments to Title 31 regulations;

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

7. Changes/amendments to Title 31 reporting forms;
8. New guidance, advisories, and/or bulletins issued by FinCEN, including frequently asked questions; and,
9. The extent to which errors and omissions to information relating to Currency Transaction Report by Casinos (CTRC)s and Suspicious Activity Report by Casinos (SARC)s occur, whether or not corrected prior to filing.

**19.5 Currency Transaction Report by Casinos (CTRC) Procedures**

Each casino shall file a report of each transaction or aggregate transactions in currency, involving either cash in or cash out, of more than Ten Thousand Dollars (\$10,000.00) in the casino's twenty-four (24) hour gaming day.

- A. Transactions in currency involving cash in include, but are not limited to:
1. Purchases of chips, tokens, and other gaming instruments;
  2. Front money deposits;
  3. Safekeeping deposits;
  4. Payments on any form of credit, including markers and counter checks;
  5. Bets of currency, including money plays;

6. Currency received by a casino for transmittal of funds through wire transfer for a customer;
  7. Purchases of a casino's check;
  8. Exchanges of currency for currency; and,
  9. Bills inserted into electronic gaming devices.
- B. Transactions in currency involving cash out include, but are not limited to:
1. Redemptions of chips, tokens, tickets, and other gaming instruments;
  2. Front money withdrawals;
  3. Safekeeping withdrawals;
  4. Advances on any form of credit, including markers and counter checks;
  5. Payments on bets;
  6. Payments by a casino to a customer based on receipt of funds through wire transfers;
  7. Cashing of checks or other negotiable instruments;
  8. Exchanges of currency for currency;
  9. Travel and complimentary expenses and gaming incentives; and,

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

10. Payment for tournament, contests, and other promotions.
- C. Casinos are exempted from reporting the following currency transactions:
1. Transactions with domestic banks;
  2. Transactions between a casino and a currency dealer or exchanger, or between a casino and a check casher, so long as such transactions are conducted pursuant to a contractual or other arrangement with a casino covering the financial services in Part (A)(8), Part (B)(7), and (B)(8) of this Section;
  3. Cash out transactions to the extent the currency is won in a money play and is the same currency the customer wagered in the money play, or cash in transactions to the extent the currency is the same currency the customer previously wagered in a money play on the same table game without leaving the table;
  4. Bills inserted into electronic gaming devices in multiple transactions (unless a casino has knowledge pursuant to the definition of 'knowledge of a cash transaction or suspicious activity' contained in Section 19.1, in which case this exemption does not apply); and,
5. Jackpots from electronic gaming devices.
- D. Prior to completing any single currency transaction in excess of Ten Thousand Dollars (\$10,000.00) or when the last transaction within a series of transactions exceeds Ten Thousand Dollars (\$10,000.00), the casino shall complete the appropriate Title 31 reporting requirements.
1. FinCEN Form 103 - Currency Transaction Report by Casinos, or any other form designated by FinCEN for reporting currency transactions in excess of Ten Thousand Dollars (\$10,000.00), shall be completed by any casino having gross annual gaming revenues in excess of One Million Dollars (\$1,000,000.00) and within this Section shall be referenced as a CTRC.
  2. IRS/FinCEN Form 8300 – Any casino that is below One Million Dollars (\$1,000,000.00) in gross annual gaming revenues and non-gaming related businesses at a casino with over One Million Dollars (\$1,000,000.00) in gross annual revenue are required to file a Form 8300 for any one transaction or aggregated cash transactions that are over Ten Thousand Dollars (\$10,000.00).
  3. CTRC forms shall be provided to all departments that may be

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

responsible for reportable transactions.

4. CTRC forms shall be completed in accordance with, and contain the information required in Title 31 for all reportable transactions.
- E. Before concluding any transaction with respect to which a CTRC report is required (i.e., before completing the currency exchange) under this Section, the handler of the transaction shall:
1. Obtain and record the complete name, date of birth (DOB), account number, and the SSN or TIN, if any, of the person or entity on whose behalf such transaction is to be effected;
  2. If the customer's Social Security Card is not available to verify identification, the customer must complete form W-9 Request for Taxpayer Identification Number and Certification;
  3. Obtain, or reasonably attempt to obtain, the customer's physical (permanent) address – Do not enter a post office box number unless the person has no physical address; and,
  4. Obtain, examine, and copy the customer's primary identification credentials, and compare to previously obtained information;
  5. Acceptable forms of primary identification include a driver's

license, military or military dependent identification card, passport, alien registration card, state issued identification card, cedular card (foreign), or other photo identification and/or combination of unexpired documents that contain an individual's name and address and are normally accepted by financial institutions as a means of identification when cashing checks for persons other than established customers;

6. This standard also applies to the agent of a customer;
7. As an option to requesting the necessary identification and other data from an established customer, information on file may be used if:
  - a. The handler of the transaction knows the customer;
  - b. The customer's name and appropriate identification credential were obtained from the customer for a previous transaction;
  - c. The information is on file to properly complete a CTRC; and,
  - d. The customer information on file is periodically updated as follows:
    - i. Copy of original identification

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

- credentials;
- ii. Copy of Social Security Card with tax identification, if any, or form W-9 Request for Taxpayer Identification Number and Certification;
  - iii. Documentation of the examinations is included in the information on file;
  - iv. Expiration dates of identification credentials are included in the information on file; and,
  - v. The transaction date is prior to the expiration date on file;
8. If a customer refuses or cannot provide the required information in this Section, the transaction shall be immediately terminated and Surveillance notified. The transaction may not be completed until the customer can comply with the requirements. In case of a dispute, casino management and the CNGC will be notified;
9. In any situation where requirements in this Section are not complied with the customer shall be barred from further gaming until a CTRC can be completed as required. For purposes of barring the customer, the description (and name, if known) of the customer is communicated to all personnel in surveillance, security, gaming or gaming related areas, the accounting department and affiliates. The casino shall use all methods available to prevent any further transactions from occurring; and,
10. Upon completion of the report, the handler of the transaction signs the CTRC and submits it to the designated department for auditing and filing. The form(s) must be sent to the designated department within twenty-four (24) hours after the end of the designated gaming day.
- F. The designated individual / department shall audit and ensure the completeness of all currency transaction reports and shall file the report in accordance with CTRC instructions.
- G. A currency transaction report for each transaction or series of transactions, in currency, involving either cash in or cash out, of more than Ten Thousand Dollars (\$10,000.00) in a gaming day must be filed with the IRS in accordance with current IRS filing deadlines. Casinos may report both cash in and cash out transactions by or on behalf of the same customer on a single currency transaction report.

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

**19.6 Structured Transactions**

- A. No person shall for the purpose of evading the transactions in currency reporting requirements of Title 31, with respect to such transaction:
1. Cause or attempt to cause the casino operation to fail to file a report required under these standards;
  2. Cause or attempt to cause a casino operation to file a report required under these standards that contains a material omission or misstatement of fact; or,
  3. Structure, attempt to structure, assist in structuring, or attempt to assist in structuring any transaction which is required to be reported under these standards.
- B. Violation of any standard set forth in this Section may result in license revocation or denial by CNGC, in addition to possible civil and/or criminal penalties as provided for under Title 31.

**19.7 Multiple Transaction Log (MTL) Procedures**

- A. Multiple currency transactions totaling more than Ten Thousand Dollars (\$10,000.00) during any gaming day are reportable under Title 31. A separate record containing a list(s) of each transaction between the casino and

its customers involving currency and having a value of Three Thousand Dollars (\$3,000.00) or more must be aggregated (kept track of) on an MTL in order to determine if the Ten Thousand Dollars (\$10,000.00) threshold has been attained.

- B. "Cash in" transactions are to be aggregated (added to) only with other "cash in" transactions. "Cash out" transactions are only to be aggregated with other "cash out" transactions unless it is a cash exchange transaction. Cash exchange transactions are "currency for currency" transactions and are recorded as both cash in and cash out.
- C. MTLs logging each currency transaction of Three Thousand Dollars (\$3,000.00) or more shall be maintained and aggregated for each gaming day.
- D. MTLs will be located at monitoring areas within each department for this purpose, and are established at each single specific cage and at each specific gaming pit or grouping of tables supervised by an individual. Such cut-off times are delineated within the system of internal control documented in the casino's Compliance Program.
- E. Alternately, an MTL may be assigned to any single cage cashier for each shift, provided the casino has established controls to account for all MTLs issued/required each gaming day.

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

F. MTL

1. An MTL is a one-part log maintained in each monitoring area, or as assigned, for purposes of recording information relative to loggable currency transactions. Only one (1) MTL is used at a time, per monitoring area or cashier, for each designated twenty-four (24) hour period (e.g. gaming day).
  2. Upon encountering the first transaction subject to MTL reporting, the handler or employee shall obtain all information required by Section 19.5(E).
  3. An MTL shall contain the following information for loggable transactions of Three Thousand Dollars (\$3,000.00) or more:
    - a. Time, date, and amount of transaction;
    - b. The name and SSN/TIN and/or other unique identification number used to establish the identity of the customer;
    - c. The type of transaction (i.e., cash in or cash out);
    - d. The name and employee identification number of the employee who conducted each transaction; and,
    - e. Signature and employee identification number of the individual responsible for the accuracy of the record.
  4. For each unknown customer, attach backup documentation (i.e., copy of primary identification, verified address, date of birth (DOB), and SSN/W-9 Form, as required). Only one (1) copy of required documentation is necessary for customers having multiple transactions within a single gaming day.
  5. Loggable transactions will be placed on the list in the chronological order in which they occur.
- G. To prevent the circumvention of the prohibitions of Title 31 or the reporting and record keeping requirements of Title 31 by multiple transactions, dissimilar cash-in transactions or dissimilar cash-out transactions, each employee and/or supervisor in each monitoring area shall:
1. Ensure MTLs are available to each designated monitoring area or cage cashier which may encounter loggable transactions;
  2. For transactions that they handle, record loggable transactions on MTLs and include the information described in Section 19.7(F)(4) for the transaction. Loggable transactions are recorded prior

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

to completing the transaction;  
and,

3. For the applicable area of responsibility:

- a. Review the MTLs and ensure that all required information has been obtained;
- b. As applicable, notify other responsible personnel that the monitoring process has been initiated for a particular customer;
- c. Sign and date the MTL as the reviewing supervisor; and,
- d. Forward to the designated individual / department responsible for aggregation with all monitoring areas within the casino.

H. At the conclusion of the designated shift for individually assigned MTLs and/or at the end of the gaming day for designated monitoring areas recording information on the previous MTL shall cease and a new MTL is started.

I. An MTL is completed for each monitoring area and/or cage cashier during the gaming day, regardless of whether or not any loggable transactions have occurred. If no loggable transactions were observed for the designated twenty-four (24) hour period, an indication such as "no

activity" is to be recorded on the MTL.

J. On a routine basis, no longer than twenty-four (24) hours after the end of a designated gaming day, MTLs are submitted to the designated individual/department to be reviewed for compliance and to complete any CTRC reporting requirements.

**19.8 Negotiable Instruments Log (NIL) and Procedures**

A. In addition to the MTLs, the casino shall maintain a separate record containing list(s) of each transaction with its customers involving the following instruments and having a face value of Three Thousand Dollars (\$3,000.00) or more:

- 1. Personal Checks;
- 2. Business Checks (including casino checks);
- 3. Official Bank checks;
- 4. Cashier's checks;
- 5. Third-party checks;
- 6. Traveler's checks; and,
- 7. Money Orders.

B. NILs shall be maintained for each type of negotiable instrument issued/received by the casino for each gaming day. Only

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

instruments approved by the CNGC may be accepted.

- C. NILs shall be maintained in each area of the casino that issues / accepts negotiable instruments.
- D. An NIL shall contain the following information for loggable transactions:
  - 1. Time, date, and amount of the transaction;
  - 2. The name and permanent address of the customer;
  - 3. The type of instrument;
  - 4. The name of the drawee or issuer of the instrument;
  - 5. All reference numbers (e.g., casino account number, personal check number, etc.);
  - 6. The name and employee identification number of the employee who conducted the transaction(s);
  - 7. Signature and employee identification of the individual responsible for the accuracy of the record; and,
  - 8. Loggable transactions will be placed on the list in chronological order in which they occur.
- E. On a routine basis, no longer than twenty-four (24) hours after the end of the designated gaming day, NILs shall be submitted to the

designated individual / department to be reviewed for compliance and maintained in accordance with Title 31 requirements and this section.

- F. At the conclusion of the gaming day for designated monitoring areas recording information on the previous NIL shall cease and a new NIL is started.
- G. Each employee and/or supervisor responsible for the NIL shall forward the NIL to the designated department responsible for compliance with Title 31 recordkeeping requirements on a routine basis, not longer than twenty-four (24) hours after the end of the designated gaming day.

**19.9 Suspicious Activity Report by Casinos (SARC) Procedures**

- A. Every casino shall file with FinCEN, to the extent and in the manner required, a report of any suspicious transaction that is relevant or that the casino operation believes to be relevant to a possible violation of law or regulation.
- B. A transaction requires reporting under the terms of this Section if it is conducted or attempted by, at, or through a casino, and involves or aggregates at least Five Thousand Dollars (\$5,000.00) in funds or other assets, and the casino knows, suspects, or has reason to suspect that the transaction (or pattern of

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

transactions of which the transaction is a part):

1. Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;
  2. Is designed, whether through structuring or other means, to evade any requirements of this Section or of any other regulations promulgated under the Title 31;
  3. Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the casino knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or,
  4. Involves use of the casino to facilitate criminal activity.
- C. An individual/department shall be designated to oversee the reporting of suspicious transactions.
- D. When an officer, employee or agent of the casino determines that a possible suspicious transaction has occurred, a SARC is prepared and submitted to the individual/department designated in the Compliance Program.
  - E. SARC forms shall be available to all departments that may encounter suspicious transactions.
  - F. A suspicious transaction shall be reported by completing a SARC and collecting and maintaining supporting documentation as required by this Section.
  - G. Within twenty-four (24) hours, upon determination that a suspicious transaction may have occurred, a completed SARC shall be forwarded to the designated individual in Part C of this Section. The designated individual shall review each SARC and supporting documentation and determine whether or not a suspicious transaction has occurred that requires the SARC to be filed with FinCEN.
  - H. The designated individual shall be responsible for ensuring that the SARC form(s) are completed in accordance with Title 31 and contain the information required for all suspicious transactions reported.
  - I. The SARC shall be filed with FinCEN as indicated in the instructions to the SARC.

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

- J. A SARC shall be filed no later than thirty (30) calendar days after the date of the initial detection by the casino of facts that may constitute a basis for filing a SARC under this Section. If no suspect is identified on the date of such initial detection, a casino may delay filing a SARC for an additional thirty (30) calendar days to identify a suspect, but in no case shall reporting be delayed more than sixty (60) calendar days after the date of such initial detection.
- K. In situations involving violations that require immediate attention, such as ongoing money laundering schemes, the casino or designated individual shall immediately notify by telephone an appropriate law enforcement authority in addition to filing a SARC within the specified time frames.
- L. The casino or designated individual may also report suspicious transactions that may relate to terrorist activity by contacting the FinCEN's Hotline at 1-866-556-3974 in addition to filing a SARC within the specified time frames.
- M. SARCs are considered confidential documents and are not to be disclosed with any individual not authorized or privy to the information contained therein (e.g., law enforcement, CNGC, designated compliance personnel, etc.). No casino, director, officer, employee, nor agent of any casino operation who reports a suspicious transaction may notify any person involved in the transaction that it has been reported.
- N. Any person subpoenaed or otherwise requested to disclose a SARC or information contained in a SARC, except where disclosure is requested by FinCEN or another appropriate law enforcement or regulatory agency, shall decline to produce the SARC or to provide any information that would disclose that a SARC had been prepared or filed, as protected under Title 31.
- O. Supporting documentation shall be identified as such and maintained by the casino, and shall be deemed to have been filed with the SARC. A casino shall make all supporting documentation available to FinCEN, appropriate law enforcement agencies, and/or Federal/State gaming regulators upon request.
- P. A copy of the original SARC shall be forwarded to the CNGC within the same filing time frame as required by FinCEN. A casino shall make all original supporting documentation available for inspection purposes upon request.
- Q. A casino is not required to file a SARC for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities.

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

**19.10 Other Transaction Types**

The following standards detail how certain financial transactions should be classified or treated for MTL and CTRC purposes.

- A. When a customer buys back with cash a check or other negotiable instrument previously tendered, the transaction is recorded on an MTL or a CTRC as “other cash-in”. Such transactions must be approved by the CNGC in accordance with Section 14.1.
- B. More than one (1) customer may be part of a reportable or loggable transaction if the persons conducting the transactions are in cooperation with one another and the transaction is designed to benefit a team of customers rather than just one (1) person. In such circumstances, customer information from all customers is included on the appropriate IRS Forms or CTRC for reporting purposes.
- C. No agent may act on behalf of another customer who is not present without express legal authority/permission (e.g., power of attorney, legal dependent, named estate executor, letter of guardianship, etc.). A copy of the legal documentation may be required in order to complete a valid traceable financial transaction (e.g., casino account deposit / withdrawal, unclaimed documented jackpot, etc.). No agent may game or conduct any financial transaction that cannot be directly traced to a customer (e.g.,

purchase/redemption of casino instruments).

- D. If in a single visit an agent conducts transactions for more than one (1) customer, then for reporting purposes customer information from all customers is included on the CTRC. If more than one (1) agent is associated with one (1) customer, transactions are aggregated for the customer with agent information from all agents included on the CTRC.
- E. Employees or officers, when performing tasks in the performance of their duties on behalf of a customer, are considered the handler of the transaction rather than an agent of the customer. Employees or officers when conducting a transaction not related to the performance of their duties but rather for their own benefit are considered a customer for a transaction (or an agent if the transaction was for another person’s benefit).

**19.11 Restricted Transactions**

- A. With respect to the following transactions, each deposit of funds, account opened or line of credit extended, a casino shall secure and maintain records of all related transactions in accordance with Title 31 requirements, as approved by the CNGC. The following transactions are restricted unless otherwise approved, and included

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

in the casino's Title 31  
Compliance Program:

1. Front money deposits;
  2. Safekeeping deposits;
  3. Individual wire transfers /  
Electronic Funds Transfers for  
deposit or credit to a casino  
account;
  4. Foreign currency; and,
  5. Credit play, including (but not  
limited to):
    - a. Marker credit;
    - b. Rim credit; and,
    - c. Call bets.
- B. Procedures for accepting these  
types of transactions, must include  
controls and processes that prevent  
any financial transactions by or on  
behalf of, that go through, or are  
made in connection with any  
individual or entity identified by  
the Office of Foreign Assets  
Control (OFAC) from occurring.  
Any attempt by an individual or  
entity to conduct such financial  
transactions shall be reported to  
OFAC in accordance with OFAC  
regulations.
- C. All cash payments must adhere to  
authorization and payment  
restrictions as specified in section  
4 – General Provisions, section 12  
– Casino Instruments and  
Exchanges, and section 14 – Cage

Operations and/or other Sections  
which may be applicable.

- D. For any deposit of funds, account  
opened or line of credit extended,  
the casino shall secure and  
maintain a record of the name,  
permanent address, and SSN/TIN  
of the person involved, prior to  
initiating any transactions.
- E. Where the deposit, account or  
credit is in the name of two (2) or  
more persons, the casino shall  
secure the information required  
above for each person having a  
financial interest in the funds.
- F. The name and address of such  
person(s) shall be verified, by the  
casino, prior to initiating any  
transactions on the account. The  
verification shall be made by  
examination of the document type  
described in 19.5(E) of this  
Section.
- G. If the customer refuses or cannot  
provide the required information in  
this Section, the transaction shall  
be immediately terminated and  
Surveillance notified. The  
transaction may not be completed  
until the customer can comply with  
these requirements. In case of a  
dispute, casino management and  
the CNGC will be notified.
- H. In addition, each casino shall  
retain:
  1. A record of each receipt  
(deposit) or credit (withdrawal)  
of funds from the account  
(including funds for

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

safekeeping or front money deposits);

2. The record shall include the name, permanent address, and SSN/TIN of the person from with whom the transaction is made, as well as the date and amount of the funds received. If the person is a non-resident alien, the person's passport number or a description of some other government document used to verify the person's identity shall be obtained and recorded;
3. A record of each bookkeeping entry comprising a debit or credit to a customer's account;
4. Each statement, ledger card or other record of each deposit account or credit account with the casino, showing each transaction to the account;
5. A record of each extension of credit in excess of Two Thousand Five Hundred Dollars (\$2,500.00). The terms and conditions of such extension of credit and repayments. The record shall include:
  - a. The customer's name, permanent address, and SSN/TIN;
  - b. The date and amount of the transaction; and,
  - c. If the customer or person for whom the credit is

extended is a non-resident alien, the casino shall obtain and record his/her passport number or description of some other government issued document used to verify his/her identify.

6. A record of each advice, request or instruction received or given by the casino for itself or another person with respect to a transaction involving a person, account, or place outside the United States. Transfers on behalf of a third party are prohibited;
7. Records prepared or received by the casino in the ordinary course of business which would be needed to reconstruct a person(s) account or to trace checks deposited with the casino through the casino's records to the bank of deposit;
8. All records, documents, or manuals required to be maintained by a casino; and,
9. All records which are prepared or used by a casino to monitor a customer's gaming activity.

**19.12 Casino Management Systems / Player Tracking Records**

- A. For the purpose of complying with Title 31 reporting requirements, if a casino has knowledge of multiple currency transactions, those transactions shall be treated as a

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

single transaction if the casino has knowledge that they are by or on behalf of any person and result in either cash in or cash out totaling more than Ten Thousand Dollars (\$10,000.00) during any gaming day.

B. Knowledge of multiple transactions below the MTL reporting requirements may occur through the use of casino management systems and/or player tracking data. If the casino system provides knowledge of multiple transactions that meet reporting requirements under these provisions, the casino shall include, within its system of internal control, the processes necessary to capture the data and determine any and all reporting requirements.

C. Player tracking records, when used as a source document for documenting cash activity and when used for the purposes of complying with Title 31, are retained for a period of five (5) years. Summary documents may be retained in lieu of original player tracking records if:

1. The established customer file (i.e., player membership file) contains all requirements listed in section 19.5(E);
2. The summary documents include at a minimum, on a daily basis, all reportable transaction information recorded on the original player tracking records;

3. Original player tracking records are retained for a minimum of thirty (30) days; and,

4. Both original and summary player tracking records are retained, if possible, when the records are used as support to a SARC.

**19.13 Record Retention**

A. A copy of any completed form required to be filed under this Section shall be retained, along with all original or business record equivalent of any supporting documentation, in chronological order for five (5) years from the date of filing and must be readily available for inspection. Summary documents may be used for inspection purposes provided original documentation can be retrieved, upon request, within three (3) business days.

B. Each completed form maintained for recordkeeping purposes under this Section shall be retained in chronological order for a minimum of five (5) years from the date prepared and must be readily available for inspection. Summary documents may be used for inspection purposes provided original documentation can be retrieved, upon request, within three (3) business days.

C. All computerized programs which would enable a person to readily access and review the records

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

described in this Section or the use of any storage media to meet the retention requirements of this Section must be approved by the CNGC.

- D. All indexes, books, programs, record layouts, manuals, formats, instructions, file descriptions, and similar materials must be submitted and on file with the CNGC.

#### 19.14 Departmental Standards

The standards in this Section apply to all departments within the gaming facility that may encounter reportable transactions, all gaming departments, including but not limited to security, surveillance, the cage, and accounting departments.

- A. Job duties and responsibilities of employees include:
1. Ensuring that restricted transactions pursuant to Title 31 do not occur;
  2. Properly recording all transactions that fall under the criteria of Title 26 and Title 31 on the appropriate forms and logs and in the manner prescribed by these standards and in accordance with the approved Compliance Program;
  3. Making a diligent effort to prevent the circumvention of the reporting and record

keeping requirements of Title 26 and Title 31;

4. Being familiar with what is considered a suspicious transaction, making a diligent effort to identify and report suspicious transaction; and,
  5. Having knowledge of Title 26 and Title 31 and the minimum internal control standards relative to the employee's job duties and the casino operation.
- B. The accounting / designated department responsible for record retention and filing requirements shall:
1. Receive CTRCs, SARCs and MTLs from the various departments and ensure that MTLs are received from all monitoring areas in accordance with established deadlines in this document.
  2. Review all documents for compliance with Title 31 and these standards. MTLs are reviewed to ensure that CTRCs were completed for all reportable transactions.
  3. Document instances of noncompliance and attempts to obtain any missing information.
  4. Ensure that all exceptions discovered through this accounting review are forwarded to appropriate personnel for follow-up.

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

5. Sign reports attesting to their review and remit to the appropriate agency.
  6. File a copy of each IRS Form for Reporting Winnings, CTRC and SARC and the original MTLs in chronological order and such documents shall be readily available for examination by appropriate regulatory and law enforcement agencies.
  7. Be independent of the generation of the documents being examined. Employees from a department other than the accounting department may perform the procedures in this standard if those employees are independent of the generation of the documents being examined and are designated in the approved Compliance Program.
- C. On a routine basis, accounting personnel shall ensure that documents, including those required by Title 26 and Title 31 and these Financial Transaction Reporting MICS, are properly maintained.

**19.15 Title 31 Compliance Officer Standards**

The Compliance Officer so designated by the casino operations under their Compliance Program pursuant to Title 31 shall:

- A. Ensure that Title 31 procedure manuals or other appropriate documentation are in place and available to employees for reference purposes when needed.
- B. Ensure that a training program is established, maintained and effective.
- C. Ensure that the system of internal control relative to Title 31 is established, maintained and effective.
- D. Review and evaluate any and all Title 31 exceptions and areas of noncompliance including reviewing internal audit and independent accountant findings. Associated follow-up is documented and maintained for inspection.
- E. The Compliance Officer may have other job duties but may not be responsible for performing financial transactions that may be reportable under these Standards.

**19.16 Training Program**

- A. A training program shall be established and maintained to instruct employees as to the requirements of Title 26 and Title 31, the Financial Transaction Reporting MICS, and the casino operations system of internal control.
- B. A training coordinator shall be established who oversees the training program. The training

SECTION 19  
FINANCIAL TRANSACTION REPORTING

---

---

coordinator may have other job duties and the Compliance Officer may function in this capacity.

- C. Records are maintained to document when training was provided, the employees receiving the training, and the content of the training session. Copies of these records shall be forwarded to the CNGC for review.
- D. Employees shall receive comprehensive training before they are permitted to function in any capacity that entails the possibility of encountering a Title 26 and/or Title 31 reporting requirement, record keeping requirement or prohibition, or performing accounting department procedures.
- E. Refresher training shall be provided at least annually and shall be documented in accordance with Part C of this Section.
- F. An individual employee may be required to attend additional comprehensive training, if deemed to have an excessive number of errors and/or omissions, in order to maintain a license issued by the CNGC.
- G. Comprehensive training shall include, but is not limited to:
  - 1. Presentation of materials relative to ensuring employees have a clear understanding of the requirements in these standards, sample forms, and any appropriate procedure manuals;

- 2. Explanation of restricted transactions, loggable transactions, reportable transactions and suspicious transactions, and reviewing the duties, responsibilities and procedures associated with each employee's position;
- 3. Review the use of MTLs;
- 4. Review the definition of a customer and agent;
- 5. Review the proper completion of IRS Forms (including which form to use for each type of reportable transaction), CTRC, and/or a SARC;
- 6. Review the definition of "established customer" and when "established customer-information on file" may be used;
- 7. Review the documentation and the records that need to be created and maintained relative to these standards; and,
- 8. Explanation of the consequences of noncompliance.

SECTION 20  
FINANCE

---

---

**20.1 Departmental Standards**

- A. The Accounting / Finance department shall adhere to all standards located throughout this document, which may or may not be referenced in this section.
- B. The Accounting / Finance department is responsible for complete analysis and reporting of all revenue.
- C. The Accounting / Finance department is responsible for reviewing, analyzing, comparing, reconciling, filing, and maintaining all source documents.
- D. Accounting responsibilities may include preparing statistical reports as required, and analyzing and documenting variances noted as a result of reviewing statistical reports. Accounting shall provide adequate procedure for investigating and documenting variances, which shall include the following requirements:
  - 1. Thresholds that require investigation;
  - 2. Designation of the job position(s) responsible for investigating the variances identified;
  - 3. Adequate segregation and independence from the transactions that resulted in the variance;

- 4. Investigation procedures to be performed (e.g. checklist) and job position(s) designated to perform them; and,
  - 5. Remedial action/follow-up to be taken based upon the results of the investigation.
- E. Alternatively, another department may be designated to perform this function in Part D, provided it is independent of the transactions used to generate statistical reports.

**20.2 General Accounting Standards**

- A. The casino operation, as approved by the Cherokee Nation Gaming Commission (CNGC), shall develop and implement accounting procedures to safeguard assets, which shall include the standards outlined in this section.
- B. When establishing the system of internal control standards (SICS) and/or procedures, the casino operation should review, and consider incorporating, other external standards such as GAAP, GAAS, and standards promulgated by GASB and FASB. In the event of a conflict between the Tribal Internal Control Standards (TICS) and the incorporated external standards, the external standards prevail. Such conflicts should be communicated and agreed to by the CNGC.
- C. Each casino operation shall prepare and maintain accurate,

SECTION 20  
FINANCE

---

---

complete, legible, and permanent records of all transactions pertaining to all revenue activities for operational accountability.

D. Each operation shall prepare and maintain general accounting records on a double-entry system of accounting in accordance with Generally Accepted Accounting Principles (GAAP), maintaining detailed, supporting, subsidiary records, including but not limited to the following:

1. Detailed records identifying revenues, expenses, assets, liabilities, and equity for each casino operation;
2. Prepare minimum bankroll calculations;
3. Detailed records of all credit items accepted by the casino operation, including, but not limited to, personal, cashier's, payroll, or traveler's checks, credit card advances, guaranteed drafts or other similar credit instruments;
4. Detailed records of any wire transfers and/or authorized Electronic Fund Transfers (EFTs) with supporting documentation, including any transfers made or accepted on behalf of a customer;
5. Records for safekeeping and/or front money deposits for which the operation is the custodian and maintains a fiduciary

responsibility over the accounting of such funds;

6. Individual and statistical game records to reflect statistical drop, statistical win, and the percentage of statistical win to statistical drop for each table game, and each type of table game, by shift, by day, cumulative month-to-date and year-to-date, and individual and statistical game records reflecting similar information for all other games;
  7. Gaming machine analysis reports, by type and by each machine, with comparative actual hold percentages to theoretical hold percentages;
  8. Journal entries prepared by the operation and by its independent accountant, and,
  9. Prepare income statements and balance sheets;
  10. Prepare appropriate subsidiary ledgers to support the balance sheet;
  11. Prepare, review, and maintain accurate financial statements;
  12. Maintain and preserve all financial records and relevant supporting documentation.
- E. Accounting methodologies shall conform to the American Institute of Certified Public Accountants (AICPA) Audit and Accounting

SECTION 20  
FINANCE

---

---

Guide in regard to any interpretations of GAAP relevant to the gaming industry.

F. Each casino operation shall establish administrative, accounting, and/or revenue audit procedures for the purpose of determining effective control over an operation's fiscal affairs. The procedures shall be designed to reasonably ensure the following:

1. Assets are safeguarded;
2. Financial records are accurate and reliable;
3. Transactions are performed only in accordance with management's general and specific authorization;
4. Transactions are recorded adequately to permit proper reporting of revenue and of fees and taxes, and to maintain accountability of assets;
5. Recorded accountability of assets is compared with actual assets at reasonable intervals and appropriate action is taken with respect of any discrepancies; and,
6. Functions, duties, and responsibilities are appropriately segregated in accordance with sound business practices by competent, qualified personnel.

G. The operation as approved by the CNGC shall develop and implement a procedure and accounting methodology for administering designated funds (i.e. player pools/pots, designated contributions/ deductions, etc.) which shall detail allowable expenses and costs deducted from designated funds.

H. In accordance with the CNGC Fee Payment policy, the casino operation shall submit all documentation necessary to support fee calculations and proof of payment for fees payable to the National Indian Gaming Commission (NIGC) and to those entities designated by Tribal-State Compact. All fee calculations must comply with the requirements set forth by the NIGC and Tribal-State Compact.

### 20.3 Accounting Plan

The operation as approved by the CNGC shall develop a detailed written accounting plan which outlines their methodology, process, and procedures regarding the preparation, review, analysis, and maintenance of statistical reports. The objective of the plan is to provide sufficient detail for each member of the accounting staff and internal audit to adequately perform their job in a consistent manner. This plan shall include at a minimum the following:

A. Job positions responsible for preparing the reports, reviewing the reports, investigating variances,

SECTION 20  
FINANCE

---

---

correcting errant information, and ensuring corrective action have been taken to correct the problem.

- B. List of source documents used to obtain meter information, actual information, and the process to prepare all reports.
- C. Procedures for the following:
  - 1. Preparing reports;
  - 2. Reviewing the reports for accuracy;
  - 3. Investigating variances that exceed the allowable threshold (includes threshold used to initiate the investigation, method of documenting variance review and investigation, and events that signal and initiate a different level of review or investigation, etc.).
  - 4. Process for correcting errant information, and;
  - 5. Identifying and communicating noncompliance issues to employees.
- D. Time frames for each step of the process (e.g. reports are prepared and reviewed within two (2) days of the drops, variances that are forwarded to management for investigation are due back to accounting within five (5) days, etc.).

- E. Controls to ensure an adequate controlled environment and proper segregation of duties (e.g., the person who prepares the reports must be someone other than the person who performs the final review of the reports).

**20.4 Gross Gaming Revenue**

- A. Gross gaming revenue is the net win from gaming activities, which is the difference between gaming wins and losses before deducting costs and expenses.
- B. For Blackjack-type, non-house banked table games and/or tournament style games, in which players compete against a common player's pool, refer to paragraph E.
- C. For gaming machines, gross revenue equals drop, less payouts and personal property awarded to customers as gaming winnings.
- D. For each counter game, gross revenue equals:
  - 1. The money accepted by the casino operation on events or games that occur during the month or will occur in subsequent months (advance sales), less money paid out during the month to customers on winning wagers (cash basis); or,
  - 2. The money accepted by the casino operation on events or games that occur during the

SECTION 20  
FINANCE

---

---

- month, plus money, not previously included in gross revenue, that was accepted by the casino operation in previous months on events or games occurring in the month, less money paid out during the month to customers as winning wagers (modified accrual basis).
- E. For each card game and any other game in which the casino operation is not a party to a wager (non-house banked games), gross revenue equals all money received by the operation as compensation for conducting the game (i.e. rake, ante, commissions, entry fee, and admission fees).
1. Expenses deducted from common pools or pots and/or other designated monies, including prizes distributed to customers and paid for by the common pool or pot, may not be deducted from gross gaming revenue.
  2. [Reserved].
- F. In computing gross revenue for gaming machines, and bingo, the actual cost to the casino operation of any personal property distributed as losses to customers may be deducted from winnings (other than costs of travel, lodging, services, food, and beverages), if the operation maintains detailed documents supporting the deduction.
- G. If the operation provides periodic payments to satisfy a payout resulting from a wager, the initial installment plan, when paid, and the actual cost of a payment plan, which is funded by the operation, may be deducted from winnings. The operation is required to obtain the approval of all payment plans from the CNGC. For any funding method which merely guarantees the casino operation's performance, and under which the operation makes payments out of cash flow (e.g. irrevocable letters of credits, surety bonds, or other similar methods), the operation may only deduct such payments when paid to the customer.
- H. For payouts by wide-area progressive/inter-casino linked gaming machine systems, a casino operation may deduct from winnings only its pro rata share of the gaming machine system payout. It is not permissible to deduct amounts to cover payments of fees, costs, or expenses associated with, or attributable to administering the inter-casino system.
- I. Cash-out tickets issued at a gaming machine or gaming device shall be deducted from gross revenue as jackpot payouts in the month the tickets are issued by the gaming machine or gaming device. Tickets deducted from gross revenue that are not redeemed within a period, not to exceed one hundred eighty (180) days of issuance, shall be included in gross

SECTION 20  
FINANCE

---

---

revenue. An unredeemed ticket previously included in gross revenue may be deducted from gross revenue in the month redeemed.

- J. If the casino pays a percentage of the revenue generated by participating gaming machines to equipment distributors or manufacturers for the use of the machines, the deduction of such payments from the amount wagered is not permitted. Total win should be recorded as revenue and the participating distribution should be recognized as an operating expense.
- K. The deduction of amounts paid to the State or other designated entity is a cost of doing business and not a payout or loss arising from a wagering transaction and is not an allowable deduction from gross gaming revenue.
- L. Promotional allowances/casino complimentaries (comps) that the casino gives to customers as an inducement to game may not be included as a deduction in the computation of gross gaming revenue. However, the retail amount of promotional allowances may be included in gross revenues and offset by deducting it from gross revenues on the face of the income statement.
- M. A casino operation may not deduct from gross revenue the unpaid balance of an approved credit instrument unless such credit is

restricted to gaming activity. Such deductions must be approved by the CNGC.

**20.5 Trial Balance – Casino Credit**

- A. Casino credit may be extended only as approved by the CNGC. No person shall be granted a loan or gifts that require remuneration to the casino operation. Personal checks, cashier's checks, payroll checks, or traveler's checks may be accepted provided they are warranted by and in accordance with procedures established by a national check clearing firm and/or as approved by the CNGC. Major credit and bank debit cards may be accepted only with proper identification and in accordance with the Bank or Credit Service requirements. Automated Teller Machines (ATMs) and Cash Access devices are exempt from these standards.
- B. A trial balance of the casino operation's accounts receivable, including the name of the customer and current balance, shall be prepared at least monthly for active, inactive, and settled or written-off accounts. The reconciliation and any follow up performed shall be documented and retained.
- C. The casino operation shall establish and comply with procedures, as approved by the CNGC, to effectively document its attempt to collect items

SECTION 20  
FINANCE

---

---

returned/refused for the full amount of the debt. Such documentation would include, but not be limited to, letters sent to the customer, logs of personal or telephone conversations, proof of presentation of the credit instrument to the customer's bank for collection, settlement agreements, or other documents which demonstrate that the operation has made a good faith attempt to collect the full amount of the debt. Such records documenting collection efforts shall be made available to the CNGC or NIGC upon request.

- D. The trial balance of the casino operation's accounts receivable shall be reconciled to the general ledger each month. The reconciliation and any follow up performed shall be documented, maintained for inspection, and provided to the CNGC upon request.
- E. A trial balance of the casino operation's inactive or written-off accounts receivable, including the customer name and balance, shall be prepared at least quarterly.

**20.6 Chart of Accounts**

- A. The operation shall periodically prescribe a uniform Chart of Accounts and accounting classifications in order to ensure consistency, comparability, and effective disclosure of financial information.

- B. The Chart of Accounts shall provide the classifications necessary to prepare the standard financial statements.
- C. The addition of new accounts must be documented and authorized by at least two (2) persons, one (1) of whom must be a management official.
- D. The prescribed Chart of Accounts shall be the minimum level of detail to be maintained for each accounting classification by the casino operation.
- E. The Chart of Accounts shall be made available to the CNGC, along with any and all revisions and additions.

**20.7 Maintenance and Preservation of Books, Records, and Documents**

- A. Each casino shall maintain complete, accurate, legible, and permanent records of all transactions pertaining to the revenues and expenses, assets, liabilities, and equity in conformance with Generally Accepted Accounting Principles (GAAP).
- B. All books, records, and documents pertaining to the conduct of wagering activities shall be retained by a casino operation in accordance with the following schedule. A record that summarizes transactions is

SECTION 20  
FINANCE

---

---

sufficient, provided that all documents containing an original signature(s) attesting to the accuracy of a related transaction are independently preserved. Original books, records, or documents shall not include copies of originals, except for the copies that contain original comments or notations or parts of multi-part forms. The following original books, records, and documents shall be retained by the casino operation for a minimum of five (5) years:

1. Casino Cage/Vault documents, including but not limited to:
  - a. All fund transfer forms for cash and cash equivalents;
  - b. Fill and Credit documentation;
  - c. Documentation for Safekeeping and Front Money deposits;
  - d. Documentation supporting increases or decreases to casino Cage inventory;
  - e. Documentation supporting changes to accounts receivable;
  - f. Deposit slips; and,
  - g. Cage accountability forms.
2. Cashier closing documentation, including but not limited to:

- a. All fund transfer forms for cash and cash equivalents;
  - b. Any and all redemptions of casino instruments, (summary reports may be used following the audit process, provided the disposition of casino instruments is approved by the CNGC);
  - c. Coupons and Vouchers (promotional payouts, player incentives, etc.);
  - d. Refunds and discounts;
  - e. Supporting documentation;
  - f. Closing summary;
  - g. Variance documentation; and,
  - h. Prize claim forms.
3. Documentation supporting the calculation of table game win, including but not limited to:
    - a. Beginning and ending Table Inventory Slips;
    - b. Fill and Credit Slips;
    - c. Requests for Fill/Credit;
    - d. Master Games reports;
    - e. Promotional payouts made from the table bank;
    - f. Table drop documentation, including table ante

SECTION 20  
FINANCE

---

---

- |   |  |
|---|--|
| <p>revenue and coupons/vouchers; and,</p> <p>g. Documentation regarding player's pool administration, including supporting documentation for calculations of direct costs and other decreases made to the pool.</p> <p>4. Documentation supporting the calculation of gaming machine win;</p> <p>a. Sales summary stating total wagers (write) and game (win) payouts;</p> <p>b. Cash-in/Ticket-in, Cash-out/Ticket out obtained through an on-line accounting system or meter readings from individual machines;</p> <p>c. Progressive and Jackpot payouts, by machine; and,</p> <p>d. Gaming machine drop documentation, including variances between drop reports/bill-in meter readings and actual count sheet and documentation to evidence investigations.</p> <p>5. Documentation supporting card room revenue;</p> <p>6. Documentation supporting tournament revenue, prize pool administration, and prize</p> | <p>payouts (if not supported by prize pool);</p> <p>7. Documentation supporting the calculation of revenue received from games of pari-mutuel, bingo, and pull-tabs;</p> <p>8. Table games statistical analysis reports;</p> <p>9. Gaming machine statistical analysis reports;</p> <p>10. Bingo, pull-tab, and pari-mutuel wagering statistical reports; and,</p> <p>11. Documentation for recording Player Tracking incentives and comps (as applicable).</p> <p>12. Internal audit documentation and reports;</p> <p>13. Documentation supporting the write-off of approved credit instruments;</p> <p>14. Supporting documentation for recording the accountability of casino assets compared to physical assets.</p> <p>15. All other books, records, and documents pertaining to the conduct of wagering activities that contain original signature(s) attesting to the accuracy of the related transaction.</p> <p>C. Documents shall be stored in a secure location, by date and shall</p> |
|---|--|

SECTION 20  
FINANCE

---

---

adhere to CNGC regulations regarding the collection, storage, preservation, and destruction of sensitive documents.

- D. Unless otherwise specified in this part, all other books, records, and documents shall be retained until such time as the accounting records have been audited by the operation's independent certified public accountants.
- E. The above requirements shall apply without regards to the medium by which the book, record, or document is generated or maintained (paper, computer-generated, magnetic media, etc.).
- F. All original books, records, and source documents shall be retained on-site or in an approved, secure location for a period of five (5) years which shall:
  - 1. Be available for inspection by agents of the CNGC during all hours of operation and/or provided within a timeframe established by said agents;
  - 2. Be maintained, organized, and indexed in such a manner so as to provide immediate accessibility to agents of the CNGC; and,
  - 3. Be destroyed only after the expiration of the minimum retention period specified or upon written request the CNGC may grant approval to permit destruction at an earlier date

for specific documents (e.g., cash-out tickets, game boards, pull tabs, etc.).

- G. Missing or incomplete documentation constitutes a violation of these standards and may result in enforcement action.

SECTION 21  
INFORMATION TECHNOLOGY

---

---

**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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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 and/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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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).

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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;

SECTION 21  
INFORMATION TECHNOLOGY

---

---

- 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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

systems and the date the use 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,

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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.

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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 alphanumeric 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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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:

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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.

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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 inbound 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.

SECTION 21  
INFORMATION TECHNOLOGY

---

---

- 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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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

SECTION 21  
INFORMATION TECHNOLOGY

---

---

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

SECTION 22  
REVENUE AUDIT

---

---

**22.1 General**

- A. Audits must be performed by employees independent of the transactions being audited.
- B. The performance of revenue audit procedures, the exceptions noted, and the follow up of all revenue audit exceptions must be documented and maintained.
- C. Controls must be established and procedures implemented to audit each operational area of the casino.

**22.2 Bingo Audit Standards**

- A. At the end of each month, verify the accuracy of the ending balance in the bingo control log by reconciling it with the bingo paper inventory. Investigate and document any variances noted.
- B. Daily, reconcile supporting records and documents to summarized paperwork or electronic records (e.g. total sales and payouts per shift and/or day).
- C. At least monthly, review variances related to bingo accounting data in accordance with an established threshold, which must include, at a minimum, variance(s) noted by the Class II gaming system for cashless transactions in and out, electronic funds transfer in and out, external bonus payouts, vouchers out and coupon promotion out. Investigate and document any variance noted.

- D. At least monthly review statistical reports for any deviations from mathematical expectations exceeding a threshold established by CNGC. Investigate and document any deviations compared to the mathematical expectations required to be submitted per CNGC Technical Standards.
- E. At least monthly, take a random sample, foot the vouchers redeemed and trace the totals to the totals recorded in the voucher system and to the amount recorded in the applicable cashier's accountability document.

**22.3 Pull Tab Audit Standards**

- A. Daily, verify the total amount of winning pull tabs redeemed each day.
- B. At the end of each month, verify the accuracy of the ending balance in the pull tab control log by reconciling the pull tabs on hand. Investigate and document any variance noted.
- C. At least monthly, compare for reasonableness the amount of pull tabs sold from the pull tab control log to the amount of pull tab sales.
- D. At least monthly, review statistical reports for any deviations exceeding a specified threshold, as defined by the CNGC. Investigate and document any large and unusual fluctuations noted.

SECTION 22  
REVENUE AUDIT

---

---

**22.4 Card Games Audit Standards**

- A. Daily, reconcile the amount indicated on the progressive sign/meter to the cash counted or received by the cage and the payouts made for each promotional progressive pot and pool. This reconciliation must be sufficiently documented, including substantiation of differences and adjustments.
- B. At least monthly, review all payouts for the promotional progressive pots, pools, or other promotions to verify payout accuracy and proper accounting treatment and that they are conducted in accordance with conditions provided to the patrons.
- C. At the conclusion of each contest/tournament, reconcile all contest/tournament entry and payout forms to the dollar amounts recorded in the appropriate accountability document.

**22.5 Gaming Promotions and Player Tracking Audit Standards**

- A. At least monthly, review promotional payments, drawings, and giveaway programs to verify payout accuracy and proper accounting treatment in accordance with the rules provided to patrons.
- B. At least monthly, for computerized player tracking systems, perform the following procedures:

- 1. Review authorization documentation for all manual point additions/deletions for propriety;
  - 2. Review exception reports, including transfers between accounts; and
  - 3. Review documentation related to access to inactive and closed accounts.
- C. At least annually, all computerized player tracking systems must be reviewed by employees independent of the individuals that set up or make changes to the system parameters. The review must be performed to determine that the configuration parameters are accurate and have not been altered without appropriate management authorization. Document and maintain the test results.

**22.6 Complimentary Services or Items Audit Standards**

- A. At least monthly, review the reports required in Section 17 – Complimentaries. These reports must be made available to those entities authorized by the CNGC or by tribal law or ordinance.
- B. [Reserved].

SECTION 22  
REVENUE AUDIT

---

---

**22.7 Audit Standards for Patron Deposit Accounts**

- A. At least weekly, reconcile patron deposit account liability (deposits  $\pm$  adjustments – withdrawals = total account balance) to the system record.
- B. At least weekly, review manual increases and decreases to/from player deposit accounts to ensure proper adjustments were authorized.

**22.8 Drop and Count Audit Standards**

- A. At least quarterly, unannounced currency counter and currency counter interface (if applicable) tests must be performed, and the test results documented and maintained. All denominations of currency and all types of cash out tickets counted by the currency counter must be tested. This test may be performed by internal audit or the CNGC. The results of these tests must be documented and signed by the employee(s) performing the test.
- B. For computerized key security systems controlling access to drop and count keys, perform the following procedures:
  - 1. At least quarterly, review the report generated by the computerized key security system indicating the transactions performed by the individual(s) that adds, deletes,

and changes users' access within the system (i.e., system administrator). Determine whether the transactions completed by the system administrator provide adequate control over the access to the drop and count keys. Also, determine whether any drop and count key(s) removed or returned to the key cabinet by the system administrator was properly authorized;

- 2. At least quarterly, review the report generated by the computerized key security system indicating all transaction performed to determine whether any unusual drop and count key removals or key returns occurred; and
  - 3. At least quarterly, review a sample of users that are assigned access to the drop and count keys to determine that their access to the assigned keys is appropriate relative to their job position.
- C. At least quarterly, an inventory of all controlled keys must be performed and reconciled to records of keys made, issued, and destroyed. Investigations must be performed for all keys unaccounted for, and the investigation documented.

SECTION 22  
REVENUE AUDIT

---

---

**22.9 Cage, Vault, Cash, and Cash  
Equivalents Audit Standards**

- A. At least monthly, the cage accountability must be reconciled to the general ledger.
- B. At least monthly, trace the amount of cage deposits to the amounts indicated in the bank statements.
- C. Twice annually, a count must be performed of all funds in all gaming areas (i.e. cages, vaults, and booths (including reserve areas)), kiosks, cash out ticket redemption machines, and change machines. Count all chips and tokens by denomination and type. Count individual straps, bags, and imprest banks on a sample basis. Reconcile all amounts counted to the amounts recorded on the corresponding accountability forms to ensure that the proper amounts are recorded. Maintain documentation evidencing the amount counted for each area and the subsequent comparison to the corresponding accounting accountability form. The count must be completed within the same gaming day for all areas.
  - 1. Counts must be observed by an individual independent of the department being counted. It is permissible for the individual responsible for the funds to perform the actual count while being observed.
  - 2. Internal audit may perform and/or observe the two counts.
- D. At least annually, select a sample of invoices for chips and tokens purchased, and trace the dollar amount from the purchase invoice to the accountability document that indicates the increase to the chip or token inventory to ensure that the proper dollar amount has been recorded.
- E. At each business year end, create and maintain documentation evidencing the amount of the chip/token liability, the change in the liability from the previous year, and explanations for adjustments to the liability account including any adjustments for chip/token float.
- F. At least monthly, review a sample of returned checks to determine that the required information was recorded by cage employee(s) when the check was cashed.
- G. At least monthly, review exception reports for all computerized cage systems for propriety of transactions and unusual occurrences. The review must include, but is not limited to, voided authorizations. All noted improper transactions or unusual occurrences identified must be investigated and the results documented.
- H. Daily, reconcile all parts of forms used to document increases/decreases to the total cage inventory, investigate any variances noted, and document the results of such investigations.

SECTION 22  
REVENUE AUDIT

---

---

**22.10 Inventory Audit Standards**

- A. At least monthly, verify receipt, issuance, and use of controlled inventory, including, but not limited to, bingo cards, pull tabs, playing cards, keys, pre-numbered and/or multi-part forms.
  
- B. Periodically perform minimum bankroll calculations to ensure that the casino operation maintains cash in an amount sufficient to satisfy the casino operation's obligations.

SECTION 23  
SURVEILLANCE

---

---

**23.1 Definitions**

Definitions used in previous and subsequent sections retain their meaning unless modified below:

**Component Failure** – any equipment malfunction (e.g., server, switch, cameras, monitors) that renders surveillance operations incapable of monitoring and/or recording required camera coverage.

**Surveillance Operations Room** – a secure location(s) in a casino operation used primarily for casino surveillance.

**Surveillance System** – a system of video cameras, monitors, recorders, video printers, switches, selectors, and other ancillary equipment used for casino surveillance.

**23.2 General**

A. The purpose of surveillance is to assist the operations and Cherokee Nation Gaming Commission (CNGC):

1. To safeguard the operations assets;
2. To deter, detect and prosecute criminal acts; and,
3. To maintain public confidence and trust that activities in a licensed gaming facility are conducted honestly and free of criminal elements and activity.

B. Surveillance Staffing

1. Tier A - operations that do not offer table or card games must, at a minimum, maintain and operate an unstaffed surveillance system in a secured location with procedures approved by the CNGC, whereby the areas under surveillance are continually recorded and monitored / reviewed periodically. Alternative controls must be defined for camera coverage that cannot conform to the camera coverage standards required by this Section.
2. For Tier B and C, the surveillance operations room must be staffed and the surveillance equipment monitored at all times by trained surveillance personnel. Surveillance and/or gaming facility management are required to provide a staffing plan, subject to CNGC approval, that provides for sufficient personnel to cover the activities being recorded/ensure effective casino surveillance. Any amendments to the approved staffing plan must be authorized by the CNGC prior to implementation.
3. No current or former Surveillance employee shall accept employment within another department within the

SECTION 23  
SURVEILLANCE

---

---

casino in which he/she is or was previously employed unless one (1) year has passed since the former surveillance employee worked in the surveillance room. Notwithstanding the foregoing, the CNGC may, upon the filing of a written petition by the employee and/or gaming facility management, waive this restriction and permit the employment of a current or former surveillance employee in a particular position after consideration of the following factors;

- a. Whether the former surveillance employee will be employed in a department or area of operation that the surveillance department does not monitor;
- b. Whether the surveillance and security systems of the gaming facility will not be jeopardized or compromised by the employment of the former surveillance employee in the particular position; and,
- c. Whether the former surveillance employee's knowledge of the procedures of the surveillance department would not facilitate the commission by any person

of irregularities or illegal acts and/or the concealment of any such actions or errors.

C. Location

The entrance to the surveillance operations room shall be located so that it is not readily accessible by unauthorized employees or the general public.

D. Access

1. Access to the surveillance operations room shall be restricted to members of the Surveillance Department, designated employees, and other persons authorized in accordance with the Surveillance department policy, which shall be approved by the CNGC.

- a. Persons authorized to enter the surveillance operations room without escort shall be listed by title. The Surveillance 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.

SECTION 23  
SURVEILLANCE

---

---

- b. Any person entering the surveillance operations room without specific authorization / access, must be escorted to the surveillance operations entrance by an employee with specific authorization/access and shall sign an entry access log that designates the date/time, duration, purpose of the visit, and the initials and employee number of the escort.
- 2. Any area with a workstation/ surveillance monitor located outside of the surveillance operations room access shall be highly restricted and must adhere to the location and access controls required by this Section.
- 3. Access, or the ability to access, the surveillance system from any location outside of the surveillance operation room, shall be approved by the CNGC. Such transmissions shall be effectively encrypted and password protected.

E. Training

- 1. The Surveillance department shall ensure staff is trained in the use of the equipment, knowledge of the games, house rules, and internal controls. Surveillance operations staff

must possess a valid gaming license.

- 2. Surveillance system personnel shall be adequately trained on the technical aspects of the system and the internal controls specific to system requirements. Only licensed, trained technicians and/or authorized vendors (with appropriate ID) shall be authorized to maintain or repair the surveillance system or its components.

**23.3 Equipment**

A. Clarity/Visibility Requirements

- 1. Adequate lighting is required in all areas where camera coverage is required. The lighting shall be of sufficient intensity to produce clear video recording and still picture production, and correct color correction (e.g. video output must demonstrate a clear picture, identifying the pips on chips, and the color and marking on cards, in existing light under normal operating conditions).
- 2. Color video recordings are required in all areas under normal operating and lighting conditions, unless otherwise approved by the CNGC.

SECTION 23  
SURVEILLANCE

---

---

3. For analog recordings / systems, no recorder shall have a recording interval of less than twenty (20) Frames Per Second (FPS).
  4. Digital video recording (DVR) systems shall be capable of storage and playback of images at thirty (30) Frames Per Second (FPS), full screen (4 Common Intermediate Format (CIF)), or an equivalent recording method, in real time resolution for all areas where gaming is conducted and where currency, coin and equivalents are counted, stored, accessed and transacted.
  5. For all other camera recordings required by this Section, a recording rate of not less than fifteen (15) FPS shall be required.
  6. All cameras required by this Section shall produce visual resolution that is adequate to satisfy the sufficient clarity/visibility standards specified.
- B. For Tier A the following equipment standards shall apply:
1. The surveillance system shall include date and time generators that possess the capability to display the date and time of recorded events on video and/or digital recordings. The displayed date and time shall not significantly obstruct the recorded view.
2. Each camera required by the standards in this Section shall be installed in a manner that will prevent it from being readily obstructed, tampered with, or disabled by patrons or staff.
  3. Each camera required by the standards in this Section shall possess the capability of having its picture recorded. The surveillance system shall include sufficient numbers of recorders to simultaneously record multiple gaming and count room activities, and record the views of all dedicated cameras and motion activated dedicated cameras.
  4. The Surveillance room equipment shall have total override capability over all other satellite surveillance equipment located outside the surveillance operation room.
  5. In the event of power loss to the surveillance system, alternative security procedures, such as additional supervisory/managerial or security personnel, must be implemented immediately.
- C. For Tier B and C – in addition to Tier A standards listed above, the following shall apply:

SECTION 23  
SURVEILLANCE

---

---

1. Each camera required by the standards in this Section shall possess the capability of having its picture displayed on a monitor and recorded. The surveillance system shall include sufficient number of monitors and recorders to simultaneously display and record multiple gaming and count room activities, and record the views of all dedicated cameras and motion activated dedicated cameras.
2. In the event of power loss to the surveillance system, an auxiliary or backup power source shall be available and capable of providing immediate restoration of power to all elements of the surveillance system that enable Surveillance personnel to observe the table games remaining open for play and all areas covered by dedicated cameras. Auxiliary or backup power sources such as a UPS System used in conjunction with a backup generator, or an alternate utility supplier, will satisfy this requirement.

**23.4 Surveillance Plan**

- A. Each gaming facility shall submit a surveillance system plan to the CNGC for approval.

- B. Any and all changes and/or modifications to the surveillance system plan, the surveillance system or any components must be approved by the CNGC prior to implementation.
- C. Each gaming facility shall have surveillance equipment (i.e. monitor and camera control unit) located within the on-site CNGC offices.
- D. The surveillance system plan must include a casino floor plan that shows the placement of all surveillance equipment in relation to the locations required by this Section (CNGC regulations and/or minimum internal controls) to be covered and a detailed description of the procedures utilized in the operation of the casino surveillance systems and its equipment. In addition, the plan may include other information, such as a preventative maintenance plan, that evidences compliance with this standard and all other surveillance policies and procedures requiring CNGC approval.
- E. If, after reviewing the written casino surveillance system plan, the CNGC determines the plan does not comply with the standards in this Section, the CNGC shall notify the licensee in writing, and the plan must be revised to comply with the standards of this Section and submit the revised plan within thirty (30) days after receipt of the

SECTION 23  
SURVEILLANCE

---

---

CNGCs written notice. Final approval of the surveillance plan will be made only after a test of the system and verification of compliance.

- F. Gaming facility management may not change the lighting, locations of table games, gaming machines, card games, or other gaming devices without the approval of the CNGC. The surveillance system and/or plan must also be adjusted, if necessary, to provide coverage required by this Section.
- G. In addition to any other recording requirements that are or may be imposed by this Section, surveillance shall record all views, activities, and locations as the CNGC Director or his/her designee may require from time to time. The subject(s) of such reviews shall not be notified and all recordings shall be communicated only to the Director or his/her designee, unless otherwise provided.
- H. Surveillance and/or gaming facility management shall submit for approval by the CNGC a written listing of those persons/vendors authorized to access and/or service the surveillance system and/or its components/equipment. Any changes to this list must first receive approval from the CNGC prior to implementation.

**23.5 Surveillance Activity Logs**

- A. Any system used to track or monitor surveillance shall be approved by the CNGC, and CNGC shall be granted read-only access to any surveillance system immediately upon request.
- B. Surveillance personnel shall maintain a log of all surveillance activities.
- C. Such log shall be maintained by Surveillance operation room personnel and shall be stored securely within the Surveillance department and shall be made available to CNGC immediately upon request.
- D. At a minimum, the following information shall be recorded in a surveillance log:
  - 1. Date;
  - 2. Time commenced and terminated;
  - 3. Activity observed or performed; and,
  - 4. The name or license credential number of each person who initiates, performs, or supervises the surveillance.
- E. Surveillance personnel shall also record a summary of the results of the surveillance of internal control

SECTION 23  
SURVEILLANCE

---

---

violation and/or any suspicious activity.

1. A summary of suspected/confirmed internal control and/or CNGC approved operational policy violations may be maintained in a separate log and submitted to the CNGC on a weekly basis.
2. The Surveillance department shall immediately notify the CNGC of discovery of any suspected crimes and/or suspicious activities pursuant to procedures prescribed by the CNGC.

F. Where ever surveillance notice is required by this document prior to commencing an activity, acknowledgement shall be provided prior to activity and notice shall be adequately documented.

G. The log must be retained for a minimum of one (1) year after the date of the last entry in it.

**23.6 Malfunction and Repair**

**A. Malfunction and Repair Log**

1. Surveillance personnel shall maintain a log or alternative procedure approved by the CNGC that documents each malfunction and repair of the

surveillance system as defined in this Section.

2. The log shall state the time, date, and nature of each malfunction, the efforts expended to repair the malfunction, and the date of each effort, the reasons for any delays in repairing the malfunction, the date the malfunction is repaired, and where applicable, any alternative camera coverage and/or security measures that were taken or activity was suspended.

3. The log must be retained for a minimum of one (1) year after the last entry in it.

B. In the event of a dedicated camera malfunction, the operation and/or the Surveillance department shall immediately, upon identification of the malfunction, provide alternative camera coverage or other security measures, such as additional supervisory or security personnel, to protect the subject activity.

C. A periodic inspection of the surveillance systems must be conducted. When a malfunction of the surveillance system is discovered reasonable effort shall be made to repair any dedicated camera malfunction required by the standards in this Section within seventy-two (72) hours after the

SECTION 23  
SURVEILLANCE

---

---

malfunction is discovered, provided that the camera is not the sole means of coverage and/or is not vital to the integrity for the area being monitored. In the case of the latter, the provisions of section (E) below shall apply. In the case of the former, the CNGC shall be notified of any camera(s) that has malfunctioned for more than twenty-four (24) hours and the alternative security measures being implemented.

- D. The surveillance plan shall provide sufficient redundancy and spare parts to ensure the surveillance system remains operational in the event of a component failure.
- E. Any component failure shall necessitate the immediate repair/replacement of the faulty unit, alternate camera coverage or suspend activity, and immediate notification to the CNGC. Repair or replacement of the equipment causing the component failure must be performed within four (4) hours from the audio and/or visual notification or upon identification of the failure. The CNGC may suspend activity if the malfunction cannot be repaired within a time frame suitable for the area being covered.
- F. In addition, any component failure that results in loss of coverage over any highly restricted areas shall require alternate live monitoring coverage by Security personnel.

**23.7 Maintenance and Testing**

- A. At various times, all surveillance equipment shall be subject to unannounced testing of minimum standards of resolution and operation by the CNGC or its designee.
- B. Upon completion of the testing, CNGC personnel shall meet with surveillance and gaming facility management to ascertain the approximate time needed to make necessary repairs and determine whether gaming may continue with live monitoring as required in Section 23.6 (B).
- C. All systems that display date and time:
  - 1. Shall be synchronized within plus or minus five (5) minutes of the surveillance system;
  - 2. Shall be synchronized or verified on a quarterly basis; and
  - 3. Any system or system failure shall be synchronized and verified.

**23.8 Video/Digital Records and Retention**

- A. Video surveillance and as required audio surveillance, at a minimum, must be retained pursuant to the following:

SECTION 23  
SURVEILLANCE

---

---

1. Gaming Areas – Thirty (30) days.
  2. Card/Table Games – Fourteen (14) days.
  3. Cage/Main Vault – Thirty (30) days.
  4. Security Offices – Thirty (30) days
  5. Non-Gaming Areas – Fourteen (14) days
  6. Gaming Facility Exterior – Fourteen (14) days
- B. A video library log, or comparable alternative procedure approved by the CNGC, shall be maintained to demonstrate compliance with the storage, identification, and retention standards required in this Section.
- C. Recordings involving suspected or confirmed gaming crimes, unlawful activity, or detentions by security personnel, must be retained for a minimum of one (1) year and until any investigation is concluded.
- D. Video files maintained for evidentiary purposes shall be adequately safeguarded and logged with the date and time it was recorded, the name of the individual who recorded it, the name and title/agency of the

person receiving the file and the date and time file was released.

- E. Duly authenticated copies of video recordings and/or digital records shall be provided to the CNGC upon request.
- F. Any video requests made by the CNGC shall be kept confidential and not be included on any distributed activity logs.

**23.9 Security**

- A. For the purpose of this section, the term “security holding room” means any room / location identified by security where an individual, whether an employee or patron that is suspected of an improper act or crime, may be held, detained, questioned, interviewed, or interrogated.
- B. The surveillance system must cover any security holding room where any person(s) may be detained, questioned, interviewed or interrogated by casino security officers. Security holding room coverage must include both audio and video, be recorded at all times that a person(s) is/are detained, questioned, interviewed or interrogated in the area. In each office or room covered by this Section, a sign must be conspicuously displayed which states that the area is under

SECTION 23  
SURVEILLANCE

---

---

constant audio and video surveillance.

- C. All Tier C gaming facilities must have a segregated room for the purpose of meeting the requirements of this section.
- D. A segregated holding room with audio surveillance is preferred for Tier A and B facilities, but is not required. However, if audio surveillance is not utilized, two (2) persons, one (1) of whom must be a member of management, shall be required to be present at any time a person(s) may be questioned, interviewed, or interrogated.

**23.10 Bingo/Pull Tabs**

- A. The surveillance system shall possess the capability to monitor the bingo ball drawing device or random number generator, which shall be recorded during the course of the drawing by a dedicated camera with sufficient clarity to identify the balls drawn or numbers selected.
- B. The surveillance system shall monitor and record the game board and the activities of the employees responsible for drawing, calling, and entering the balls drawn or numbers selected.
- C. Pull Tabs

- 1. The sale of pull tabs at a Point of Sale (POS) and/or vending machine shall follow standards out lined in Section 23.17.
- 2. Pull tabs and/or similar inventory shall be monitored in accordance with Section 23.21.

**23.11 Gaming Machines**

- A. Except as otherwise provided in paragraphs 23.11 (B) and (C) of this Section, any gaming machines offering a payout of more than Two Hundred and Fifty Thousand Dollars (\$250,000.00) or those with a minimum wager of Twenty-five Dollars (\$25.00) or more shall be monitored and recorded by a dedicated camera(s) to provide coverage of:
  - 1. All guests and employees at the gaming machine; and,
  - 2. The face of the gaming machine, with sufficient clarity to identify the payout line(s) of the gaming machine.
- B. In-house progressive gaming machines offering a base payout amount (jackpot reset amount) of One Hundred Thousand Dollars (\$100,000.00) or more shall be recorded by a dedicated camera(s) to provide coverage of:
  - 1. All guests and employees at the gaming machine; and,

SECTION 23  
SURVEILLANCE

---

---

2. The face of the gaming machine, with sufficient clarity to identify the payout line(s) of the gaming machine.
  3. Progressive prize meters.
- C. Wide-area progressive:
1. Wide-area progressive gaming machines offering a base payout amount of One Million Dollars (\$1,000,000.00) or more and monitored by an independent vendor utilizing an on-line progressive computer system shall be recorded by a dedicated camera(s) to provide coverage of:
    - a. All customers and employees at the gaming machine; and,
    - b. The face of the gaming machine, with sufficient clarity to identify the payout line(s) of the gaming machine.
    - c. Progressive prize meters.
  2. Any standards a vendor may require must be submitted to CNGC for review and approval, prior to installation.
- D. For linked/grouped gaming machines utilized for tournament offerings, the surveillance system shall provide at a minimum one (1) pan, tilt, and zoom (PTZ) camera

with sufficient clarity to identify all customer and employee activities at the gaming machine tournament area.

- E. Notwithstanding paragraph 23.11 (A) of this Section, if the gaming machine is a progressive or multi-game machine, the CNGC, or the operations subject to the approval of the CNGC, may develop and implement alternative procedures to verify payouts.

**23.12 Table Games**

- A. The surveillance system of operations operating four (4) or more table games shall provide at a minimum one (1) PTZ camera per two (2) tables and one (1) dedicated camera capable of recording:
  1. With sufficient clarity to identify customers and dealers; and,
  2. With sufficient coverage and clarity to simultaneously view the table bank and determine the configuration of wagers, card values, and game outcome.
- B. One (1) dedicated camera per table and one (1) PTZ camera per four (4) tables may be an acceptable alternative procedure to satisfy the requirements of subsection (A) in this standard.

SECTION 23  
SURVEILLANCE

---

---

C. The surveillance system of operations operating three (3) or fewer table games shall:

1. Comply with the requirements of paragraph 23.12 (A) of this Section; or
2. Have one (1) overhead camera at each table.

D. Table games with a guaranteed base jackpot of Twenty-five Thousand Dollars (\$25,000.00) or more shall be recorded and monitored by dedicated cameras that provide coverage of the following:

1. The table surface sufficient that the card values and card suits can be clearly identified.
2. An overall view of the entire table with sufficient clarity to identify customers and dealers.
3. A view of the progressive meter jackpot amount. If several tables are linked to the same progressive jackpot meter, only one (1) meter need be recorded.

**23.13 Card Games**

A. The surveillance system shall utilize one (1) dedicated camera per table for live games capable of recording:

1. With sufficient clarity to identify card games activities, including customers and dealers; and,
2. With sufficient coverage and clarity to simultaneously view the dealer's bank and determine, to the extent possible, card values, cash/cash equivalents and game outcome.
3. An unobstructed view of all posted progressive pool amounts.

B. One (1) PTZ camera per four (4) tables shall be used to monitor and record the general activities in each card room and be capable of identifying the employees performing the different functions.

**23.14 Craps/Roulette**

- A. All craps tables shall have two (2) dedicated cross view cameras covering both ends of the table.
- B. All roulette areas shall have one (1) overhead dedicated camera covering the card shuffler/reader and shall also have one (1) dedicated camera covering the play of the table.

**23.15 Tournaments**

A. Tournaments shall adhere to requirements in Sections 23.11 (D)

SECTION 23  
SURVEILLANCE

---

---

Gaming Machines, 23.12 (B) Table Games, and 23.13 (B) Card Games.

- B. Mobile / wireless cameras may be used to meet this standard, provided they are approved by the CNGC prior to installation and/or included within the Surveillance Plan.

**23.16 Pari-Mutuel Wagering**

- A. The surveillance system shall monitor and record a general overview and activities occurring in the betting station area with sufficient clarity to identify ticket writer/cashier and customers.
- B. Each betting station shall be equipped with one (1) dedicated overhead camera covering the transaction area.
- C. The surveillance system shall provide an overview of all wagering/cash transactions. This overview shall include the customer, the employee and kiosk, and the surrounding area.

**23.17 Point of Sale (POS) / Kiosks**

The surveillance system shall monitor and record a general overview of activities occurring in each area where monetary and/or non-monetary transactions are conducted with sufficient clarity to identify employees and customers.

A. Stationary POS / Manned Kiosk / Players Club

- 1. Each cashier station shall be equipped with one (1) dedicated overhead camera covering the transaction area.
- 2. The surveillance system shall provide an overview of cash and/or cash equivalent transactions.
- 3. This overview should include the customer, the employee, and the surrounding area with sufficient clarity to confirm the amount of each cash transaction.

B. Mobile POS

- 1. The surveillance system shall provide an overview of cash and/or cash equivalent transactions.
- 2. This overview should include the customer, the employee, and the surrounding area.

C. Electronic Kiosks

- 1. Each kiosk shall be equipped with one (1) dedicated camera with sufficient clarity to identify the customer conducting the transactions.
- 2. Surveillance shall be notified prior to access to the electronic kiosks.

SECTION 23  
SURVEILLANCE

---

---

**23.18 Main Cage / Vaults / Soft Count / Drop and Issue**

**A. Cage / Vault / Soft Count**

1. The surveillance system shall monitor and record a general overview of activities occurring in each cage and vault area with sufficient clarity to identify employees within the cage and customers and employees at the counter areas.
2. Each cashier station shall be equipped with one (1) dedicated overhead camera covering the transaction area.
3. The surveillance system shall provide an overview of cash transactions. This overview should include the customer, the employee, and the surrounding area.

**B. Fills and Credits**

1. The cage or vault area in which fills and credits are transacted shall be monitored and recorded by a dedicated camera or motion activated dedicated camera that provides coverage with sufficient clarity to identify the chip values and the amounts on the Fill and Credit slips.
2. Controls provided by a computerized fill and credit

system may be deemed an adequate alternative to viewing the Fill and Credit slips.

**C. Currency and Coin**

1. The surveillance system shall monitor and record with sufficient clarity all areas where currency or coin may be stored or counted.
2. The surveillance system shall provide for:
  - a. Coverage of currency counters shall be sufficiently clear to view any attempted manipulation of the recorded data.
  - b. Monitoring and recording of the table game drop box storage rack or area by either a dedicated camera or a motion activated camera.
  - c. Monitoring and recording of soft count room, including all doors to the room, all table game drop boxes, safes, and counting surfaces, and all count team personnel. The counting surface area must be continuously monitored and recorded by a dedicated camera during the soft count.

SECTION 23  
SURVEILLANCE

---

---

- d. Audio capability of the soft count room shall also be maintained.
  - e. Monitoring and recording of all areas where currency is sorted, stacked, counted, verified, or stored during the soft count process.
3. The surveillance system shall monitor and record a general overview of the activities occurring in each gaming machine cashiers station.

**23.19 Promotional Drawings and Devices**

- A. For promotional drawings with a prize value (in total) of One Thousand Two Hundred Dollars (\$1,200.00) or more, the following standards shall apply:
- 1. For any manual hopper, a dedicated camera or PTZ camera with sufficient coverage and clarity to identify customers and/or employees accessing or dropping drawing tickets for the duration of the promotion.
  - 2. For electronic drawings, a dedicated camera or PTZ camera with sufficient coverage and clarity to oversee the execution of the drawing(s).

- B. For promotional devices utilized to determine the outcome of any promotional offer (e.g. random number generator (RNG) devices, promotional kiosks, promotional gaming devices, etc.), a dedicated camera or PTZ camera with sufficient coverage and clarity to identify customers and device output during times that the device is active.

**23.20 Information Technology (IT) Data Facilities**

- A. The surveillance system shall monitor and record a general overview of activities occurring in each IT data facility where any personnel, contractor, temporary employee, and/or vendor employees perform work in or use IT data facilities.
- B. Designated IT data facilities containing IT equipment will be secured and protected from unauthorized physical access as follows:
- 1. Designated IT data facilities/equipment include but are not limited to:
    - a. Communication Equipment;
    - b. Main Distribution Frame (MDF) Closets;

SECTION 23  
SURVEILLANCE

---

---

- c. Intermediate Distribution Frame (IDF) Closets;
  - d. Information Technology Data Center;
  - e. Servers;
  - f. Workstations requiring secure access;
  - g. Electronic Gaming Systems; and,
  - h. Any other secured IT area
2. The entrance to the surveillance server and gaming server rooms shall be located so that it is not readily accessible by either casino operation employees who work primarily on the casino floor or the general public.
3. Access to all IT data facilities shall be controlled using swipe badges, in addition to a manual log that each person must sign, for those persons that do not have authorized access in accordance with CNGC Key and Access Control Standards.
4. All IT data facilities shall have surveillance coverage on all doors accessing the IT data facility and surveillance coverage for the server racks.
5. All vendors requiring access to IT data facilities shall have an

escort that must remain with them for the duration of their work in the server room. Surveillance shall be notified before vendors enter IT data facilities and entry/exit shall be logged in using the standards in 23.2 (D).

6. Access to IT data facilities shall be limited to authorized personnel and shall apply to 23.2 (D).

**23.21 Warehouse / Other Areas**

- A. Any area used for the storage of inventory shall be monitored by Surveillance, and shall contain a general overview of the stored items, or the shelving, cages, boxes, etc. with sufficient clarity to identify employees and vendors who access the area.

- 1. Storage for non-controlled items may include but not be limited to areas such as storage closets, storage room, warehouse and other facilities and/or buildings.
- 2. Any access to the secured storage containers that store controlled items (e.g. ticket paper, cards, chips, felts, players club cards, etc.) require:
  - a. Surveillance shall be notified of any access to the

SECTION 23  
SURVEILLANCE

---

---

storage area of controlled items and confirmation shall be provided prior to entry;

- b. A Security Officer must be physically present;
- c. The individuals accessing the secured items must be identified by name, position, employee number, and purpose for entry;
- d. Access to secured items shall be logged by Surveillance and/or Security Operations and made available to CNGC for review upon request; and,
- e. If the storage container is portable, notification shall be provided to the CNGC prior to moving/relocating the container. A CNGC Agent shall confirm camera coverage for compliance prior to the utilization of the new storage location.

B. The surveillance system shall monitor and record non-public areas with sufficient clarity to identify employees and/or vendors, their general activities, and be able to determine the movements/access routes they may take during the process of their duties. Surveillance shall include, but not be limited to, the following areas:

- 1. Hallways;
- 2. Break Rooms;
- 3. Employee Lockers;
- 4. Kitchens;
- 5. Food and Beverage Storage;
- 6. Storage for Alcohol/Beer; and,
- 7. Entrances/Exits

SECTION 24  
INTERNAL AUDIT

---

---

**24.1 Departmental Standards**

- A. Internal audit personnel shall immediately notify the Cherokee Nation Gaming Commission (CNGC) and the Cherokee Nation Marshal Service (CNMS) of the discovery of any violation or suspected violation of any criminal statute.
- B. An internal audit division shall report directly to the CNGC and/or evaluate compliance on behalf of the CNGC, on all areas of regulatory oversight.
- C. The internal audit division shall be sufficiently staffed to meet the regulatory audit requirements for all CNGC licensed casino operations.
- D. Internal auditor(s) are independent of casino operations with respect to the departments subject to audit.
- E. The operation may maintain a separate internal audit function, and may provide audit reports for review and consideration in meeting the required regulatory audits provided:
  - 1. The internal audit function shall be organizationally independent and shall report to a level within the organization that allows for objective performance of the appraisal function, free from undue constraint and conflicts of interests.

- 2. Internal audit personnel shall refrain from assessing specific operations for which they were previously responsible for at least one (1) year.
- 3. Internal audit personnel shall possess the knowledge, skills, and other competencies necessary to perform compliance audits.

**24.2 Reliance on Internal Auditors**

- A. External auditors may rely upon the work of internal auditors to the extent allowed by the professional standards, as set forth in Section 2.7 – Compliance, CPA Testing and Guidelines.
- B. The CNGC may rely upon the internal audit work performed by the internal audit personnel of the casino operation, as designated by the Tribal Enterprise, provided that:
  - 1. The personnel adhere to “International Professional Practices Framework ‘Redbook’ Standards” promulgated by the Institute of Internal Auditors (IIA).
  - 2. The department evaluates compliance to those standards set forth in this document and all other regulatory standards promulgated or within the oversight of the CNGC. The

SECTION 24  
INTERNAL AUDIT

---

---

internal audit department shall utilize the CNGC TICS checklist or comparable testing procedures to evaluate compliance.

3. Findings shall be reported separately for each licensed casino operation.
4. The Audit Opinion/Conclusion shall coincide with the criteria set forth by the CNGC Internal Audit division.
5. Audit work papers shall be made available immediately to the CNGC upon request .
6. The audit report must describe all instances of compliance violations and/or procedural noncompliance (regardless of materiality) with the CNGC TICS or approved variances. Source documentation shall be tested through attribute sampling and testing methods and additional findings reported based upon a sufficient number of exceptions detrimental to the effectiveness of the control policy or procedure.
7. The audit report shall contain the following information:
  - a. The citation of the applicable TICS, Regulation, and/or the control policy or procedure

for which the instance of noncompliance was noted;

- b. A narrative description of non-compliance, including the number of exceptions and the sample size tested and the probable cause (as applicable);
- c. All required compliance audits shall adhere to the *Internal Audit Guidelines* promulgated by the NIGC; and,
- d. All other reporting and documentation requirements as set forth in part 24.4 and 24.5 of this section.

### 24.3 Audits

- A. Controls must be established and procedures implemented to ensure that internal audit personnel perform audits of all major gaming areas of the casino operation.
- B. At a minimum, audits shall include compliance testing to the TICS, SICS, and NIGC MICS. The following shall be reviewed at least annually:
  1. Live Bingo - including, but not limited to: Supervision, bingo card control, bingo sales, draw, electronic equipment/ aids, payout procedures, cash and cash equivalent controls,

SECTION 24  
INTERNAL AUDIT

---

---

- |   |   |
|---|---|
| <p>operations, and revenue audit procedures and reconciliation processes;</p> <p>2. Pull tabs - including, but not limited to: Supervision, pull tab operating funds, statistical records, winner verification, perpetual inventory, accountability of sales versus inventory, and revenue audit procedures;</p> <p>3. Card games – including, but not limited to: Supervision, card game operations, exchange or transfer procedures, playing cards, reconciliation of card room bank, posted rules, promotional and progressive pots/pools, tournament activities, and count procedures;</p> <p>4. Pari-Mutuel Wagering – including, but not limited to: Write and payout procedures and pari-mutuel auditing procedures.</p> <p>5. Table games – including, but not limited to: Fill and credit procedures, play procedures, , location and control over sensitive keys, the tracing of source documents to summarized documentation and accounting records, and reconciliation to restricted copies;</p> <p>6. Gaming machines – including, but not limited to: Jackpot</p> | <p>payouts, gaming machine cabinet access, tracing of source documents to summarized documentation and accounting records, reconciliation to restricted copies, location and control over sensitive keys, compliance with software security controls and compliance with all applicable TICS procedures;</p> <p>7. Cage and Main Vault - cash and cash equivalent procedures, including, but not limited to: Supervision, all cage funds transfer procedures, cash and cash equivalents, including all checks, credit instruments, and casino instruments and exchanges, cage and vault accountability, kiosks, promotional payouts, drawings, and giveaways, and cage and vault access, and the reconciliation of trial balances to physical instruments on a sample basis. Cage accountability shall be reconciled to the general ledger;</p> <p>8. Information Technology - functions including, but not limited to: Supervision, gaming and critical systems' logical and physical controls, independence, physical security, logical security, user controls, installations and/or modifications, remote access, incident monitoring and reporting, data back-ups,</p> |
|---|---|

SECTION 24  
INTERNAL AUDIT

---

---

- software downloads, and verifying downloads, and compliance with all applicable TICS procedures;
9. Marketing Promotions and Player Tracking - including but not limited to: Supervision, promotion rules, player tracking systems and procedures, and procedures whereby promotional items are issued, authorized, and redeemed; and,
10. Complimentary Items /Services - including, but not limited to: Procedures for issuing, authorizing, redeeming and reporting comps;
11. Patron Deposit Accounts and Cashless Systems - including, but not limited to: Supervision, patron deposits, withdrawals, and adjustments;
12. Drop and Count - including, but not limited to: Supervision, count room access, drop and count team, bill acceptor/canister and drop box drop/count standards and subsequent transfer of funds, casino instrument count standards, unannounced testing of count room currency counters and/or currency interface, and controlled keys and compliance with all applicable TICS procedures; and,
13. Accounting – including, but not limited to: Accounting records, maintenance and preservation of financial records and relevant supporting documentation.
14. Any other internal audits as required by the CNGC.
- C. IRS Reporting requirements and Title 31 audits shall be reviewed at least once during each six (6) month period as outlined in part 24.8 of these standards.
- D. In addition to the observations and examinations performed under paragraph (B) of this section, follow-up observations and examinations shall be performed to verify that corrective action has been taken regarding all instances of noncompliance cited by internal audit, the independent accountant, and/or the CNGC. The verification shall be performed within six (6) months following the date of notification.
- E. Whenever possible, internal audit observations shall be performed on an unannounced basis (i.e., without the employees being forewarned that their activities will be observed). Additionally, if the independent accountant also performs the internal audit function, the accountant shall perform separate observations of the table games/gaming machine drops and counts to satisfy the internal audit observation

SECTION 24  
INTERNAL AUDIT

---

---

requirements and independent accountant tests of controls as required by the American Institute of Certified Public Accountants guide.

**24.4 Documentation**

- A. Documentation (e.g., checklists, programs, reports, etc.) shall be prepared to evidence all internal audit work performed as it relates to with the TICS, SICS, and NIGC MICS or other regulatory requirements, including all instances of noncompliance.
- B. The Internal Audit department shall operate with audit programs, which, at a minimum, address the TICS. Additionally, the department shall properly document the work performed, the conclusions reached, and the resolution of all exceptions.

**24.5 Reports**

- A. Reports documenting audits performed shall be submitted to the CNGC and maintained and made available to the NIGC, upon request, following any and all reviews pertaining to casino operations.
- B. Such audit reports shall include the following information:
  - 1. Audit objectives;

- 2. Audit procedures and scope;
- 3. Findings and conclusions;
- 4. Recommendations, if applicable; and,
- 5. Management's response.

- C. Audit reports and supporting documentation shall be retained for a period of five (5) years.

**24.6 Material Exceptions**

All material exceptions resulting from internal audit work shall be investigated and resolved with the results of such being documented and retained for five (5) years.

**24.7 Role of Management**

- A. Internal audit findings shall be reported to management.
- B. Management shall be required to respond to internal audit findings, in accordance with established deadlines, stating corrective measures to be taken to avoid recurrence of the audit exception.
- C. Failure to meet reasonably established deadlines for responses to audit findings may result in an adverse audit opinion, in addition to license suspension and/or fee, as deemed appropriate by the CNGC.
- D. Such management responses shall be included in the internal audit

SECTION 24  
INTERNAL AUDIT

---

---

report that will be delivered to management and the CNGC.

**24.8 Financial Transactions**

A. Internal audit procedures shall be performed twice each calendar year to determine compliance with the provisions of Title 26 and Title 31 and the provisions of the Minimum Internal Control Standards relative to these requirements. Procedures, at a minimum, shall include:

1. Reviews of established procedures in effect for all departments, and
2. An examination of all types of documents prepared pursuant to Title 26 and Title 31 and the Financial Transaction Reporting Tribal Internal Control Standards (TICS).

B. Audit programs for the semi-annual reviews shall include:

1. Compliance walk-through of those departments where financial transactions may occur, including interviews with employees who handle transactions;
2. General observation of accounting procedures;
3. Sufficient procedures to address the identification and reporting procedures for

reportable transactions that may occur as the result of single, multiple and/or dissimilar transaction;

4. Examination of Title 26 and Title 31 documentation including IRS Forms for reporting gambling winnings, CTRCs, SARCs, and MTLs; and,
5. Examinations of forms and supporting documentation shall include the following, (examinations may be done on a sample basis):
  - a. IRS Forms have been completed and filed for reportable transactions;
  - b. Withholdings have been accurately calculated and submitted;
  - c. CTRCs were completed and filed for reportable cash transactions;
  - d. SARCs were completed and filed for transactions that were classified as suspicious transactions;
  - e. The information contained within the CTRCs and SARCs was complete; and
  - f. No prohibited transactions have occurred.

SECTION 24  
INTERNAL AUDIT

---

---

6. An evaluation of the established system of internal controls and the procedures in effect.
  
- C. The performance and the results of the above internal audit procedures shall be documented. All exceptions discovered are also documented and forwarded to management (i.e., departments responsible for the noncompliance). The department heads are responsible for ensuring that corrective action is taken.
  
- D. Internal Audit will perform follow-up observations and examinations to verify that corrective action has been taken.