# 25 CFR § 543.20 Toolkit

# Information Technology

NIGC Training Division

Edition 02/05/2026

## Introduction

In 1988, Congress adopted the Indian Gaming Regulatory Act (IGRA) to provide a statutory basis for gaming by Indian Tribes. The National Indian Gaming Commission (NIGC) was created by IGRA to regulate gaming activities conducted by sovereign Indian Tribes on Indian lands. The mission of NIGC is to fully realize IGRA's goals of: (1) promoting Tribal economic development, self-sufficiency, and strong Tribal governments; (2) maintaining the integrity of the Indian gaming industry; and (3) ensuring that Tribes are the primary beneficiaries of their gaming activities. One of the primary ways NIGC does this is by providing training and technical assistance to Indian Tribes and their gaming regulators.

NIGC is pleased to present this toolkit to all compliance and auditing staff. This reference guide is intended to assist IT auditor(s), gaming commissioner(s), and operations' personnel in measuring compliance of their operation(s) with 25 CFR § 543.20. The toolkit provides each standard of § 543.20, the intent of the standard, and suggested minimum testing steps. Auditing to the intent and following the suggested testing steps will help reach regulatory compliance.

This toolkit is designed to meet the NIGC Minimum Internal Control Standards (MICS) and does not account for the operations' Tribal internal control standards (TICS) and/or system of internal control standards (SICS), which may require further testing. NIGC encourages operations to develop standards that exceed the MICS because each operation is unique; therefore, a robust set of controls is warranted.

If you have questions or comments about this guide, please contact the NIGC Training Program at TrainingInfo@nigc.gov. For more information, visit NIGC's website at www.nigc.gov.

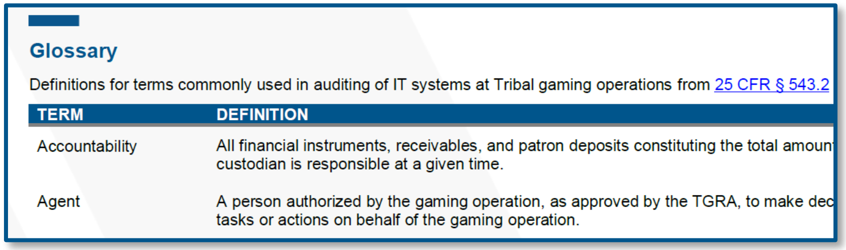
## Table of Contents

Click a section below to jump to the topic.

## How to Use This Toolkit

The NIGC Training Department has designed this toolkit as a resource for understanding 25 CFR § 543.20 *What are the minimum internal control standards (MICS) for information technology and information technology data?* It can be used as a tool when conducting an audit of Information Technology (IT) systems and data to determine compliance with the regulation. The toolkit provides many practical and concrete suggestions for understanding and evaluating compliance with the regulation for both experienced and new auditors during any stage of the auditing process.

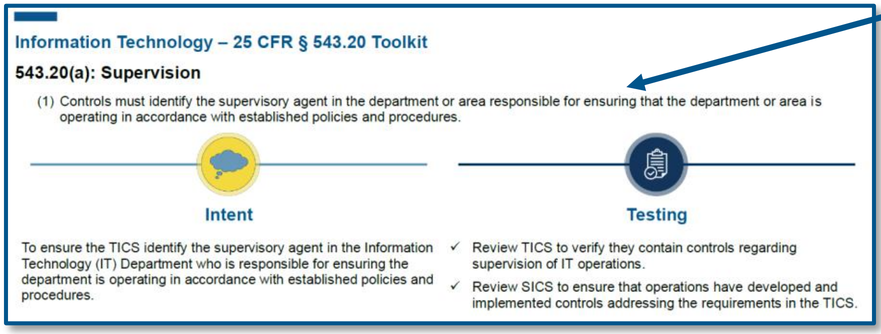
See the call outs below for what can be found in each section of the toolkit.



### Glossary

Definitions for terms commonly used in auditing of IT systems at Tribal gaming operations from 25 CFR § 543.2

| TERM | DEFINITION |
|---|---|
| Accountability | All financial instruments, receivables, and patron deposits constituting the total amoun custodian is responsible at a given time. |
| Agent | A person authorized by the gaming operation, as approved by the TGRA, to make dec tasks or actions on behalf of the gaming operation. |



Information Technology – 25 CFR § 543.20 Toolkit

**543.20(a): Supervision**

(1) Controls must identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures.

**Intent**

To ensure the TICS identify the supervisory agent in the Information Technology (IT) Department who is responsible for ensuring the department is operating in accordance with established policies and procedures.

**Testing**

- ✓ Review TICS to verify they contain controls regarding supervision of IT operations.
- ✓ Review SICS to ensure that operations have developed and implemented controls addressing the requirements in the TICS.

**Glossary** Definitions of terms commonly used in this toolkit.

**Regulation** The verbatim language of each section in 25 CFR § 543.20.

**Intent** The purpose of the regulation and the importance of the control.

**Testing** Suggested testing steps to evaluate compliance.

## Glossary

Definitions for terms commonly used in auditing of IT systems at Tribal gaming operations from 25 CFR § 543.2 and other sources.

| TERM | DEFINITION |
|---|---|
| Accountability | All financial instruments, receivables, and patron deposits constituting the total amount for which the bankroll custodian is responsible at a given time. |
| Agent | A person authorized by the gaming operation, as approved by the TGRA, to make decisions or perform assigned tasks or actions on behalf of the gaming operation. |
| Casino management system | A software platform that allows digital management of the core operations functions in a gaming operation. It can have functions that integrate various departments which could include the gaming floor, finance, and security. |
| Class II gaming | Games of chance such as bingo (whether or not electronic, computer, or other technological aids are used in connection therewith in), pull tabs, and non-banked card games (poker). |
| Class II gaming system | All components, whether or not technologic aids in electronic, computer, mechanical, or other technologic form, that function together to aid the play of one or more Class II games, including accounting functions mandated by these regulations or part 547 of this chapter. |
| Independent | The separation of functions to ensure that the agent or process monitoring, reviewing, or authorizing the controlled activity, function, or transaction is separate from the agents or process performing the controlled activity, function, or transaction. |
| Logical access control system | An automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application, or database. A logical access control system requires the validation of an individual's identity through some mechanism, such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different individuals depending on their roles and responsibilities in an organization. (NIST) |
| Kiosk | A device capable of redeeming vouchers and/or wagering credits or initiating electronic transfers of money to or from a patron deposit account. |
| MICS | Minimum internal control standards in this part. |

### 543.20(a): Supervision

| TERM | DEFINITION |
|---|---|
| Multi-factor authentication (MFA) | Authentication using two or more factors to achieve authentication. Factors are (i) something you know (e.g., password/personal identification number); (ii) something you have (e.g., cryptographic identification device, token); and (iii) something you are (e.g., biometric). (NIST) |
| Patron | A person who is a customer or guest of the gaming operation and may interact with a Class II game. May also be referred to as a “player". |
| Player tracking system | A program that allows gaming operations to track player activity and rewards players for spending money or gaming at the operation. A common structure for player rewards allows players to collect points while playing casino games. These points can then be exchanged for cash, free play, or prizes. (McGowan, 2021) |
| SICS | System of internal control standards; an overall operational framework for a gaming operation that incorporates principles of independence and segregation of function, and is comprised of written policies, procedures, and standard practices based on overarching regulatory standards specifically designed to create a system of checks and balances to safeguard the integrity of a gaming operation and protect its assets from unauthorized access, misappropriation, forgery, theft, or fraud. |
| TGRA | Tribal gaming regulatory authority, which is the entity authorized by tribal law to regulate gaming conducted pursuant to the Indian Gaming Regulatory Act. |
| TICS | Tribal Internal Control Standards established by the TGRA that are at least as stringent as the standards set forth in this part. |
| User | Individual or (system) process authorized to access an information system. (NIST) |
| User group | A collection of users with shared permissions to an information system with similar roles, responsibilities, or tasks to perform. |
| Virtual private network (VPN) | A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. (NIST) |
| Voucher | A financial instrument of fixed wagering value, usually paper, that can be used only to acquire an equivalent value of cashable credits or cash through interaction with a voucher system. |

## Sources

McGowan, S. (2021, August 5). Understanding player tracking systems. *G&M News*. https://g-mnews.com/en/understanding-player-tracking-systems/

National Institute of Standards and Technology (NIST). (n.d.). Glossary. *Computer Security Resources*. https://csrc.nist.gov/glossary

## Information Technology – 25 CFR § 543.20 Toolkit

### 543.20(a): Supervision

(1) Controls must identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures.

### Intent

To ensure the TICS identify the supervisory agent in the Information Technology (IT) Department who is responsible for ensuring the department is operating in accordance with established policies and procedures.

### Testing

- ✓ Review TICS to verify they contain controls regarding supervision of IT operations.
- ✓ Review SICS to ensure that operations have developed and implemented controls addressing the requirements in the TICS.

## 543.20(a): Supervision

(2) The supervisory agent must be independent of the operation of Class II games.

### Intent

To ensure the duties of IT supervisory agents are separate from those in charge of Class II gaming systems, including but not limited to Class II servers, player interfaces, and player tracking.

### Testing

- ✓ Review casino operations' organizational chart to determine if the supervisory agent(s) over IT are independent of the operation of Class II games.
- ✓ Inquire with IT supervisory agent(s) to identify to whom they report.

## 543.20(a): Supervision

(3) Controls must ensure that duties are adequately segregated and monitored to detect procedural errors and to prevent the concealment of fraud.

### Intent

To ensure IT agents are not given duties that give them access to financial instruments, accounting, audit, ledger entries, or payout forms. Keeping these roles separate and making sure they are monitored helps prevent fraud and detect errors.

### Testing

- ✓ Review job descriptions and user access permissions for IT agents, including user groups, to verify the appropriate role(s) and user group(s) to which IT agents should be assigned.
- ✓ Review the user groups to which IT agents belong and verify the level of access permissions are appropriate for the job description or title. Flag instances of access to financial, accounting, or gaming roles (e.g., financial systems, accounting systems, player tracking).

## 543.20(a): Supervision

(4) Information technology agents having access to Class II gaming systems may not have signatory authority over financial instruments and payout forms and must be independent of and restricted from access to:

(i) Financial instruments;

(ii) Accounting, audit, and ledger entries; and

(iii) Payout forms.

### Intent

To ensure IT agents who have access to Class II gaming systems are not allowed to handle or approve financial instruments; accounting audit, and ledger entries; and payout forms to prevent conflicts of interest and protect the integrity of financial operations.

### Testing

- ✓ Review SICS to verify that IT personnel are not authorized to approve financial transactions such as payout forms.
- ✓ Review system user access accounts of IT personnel to determine if they have access to financial, accounting, ledger, payout forms, player tracking bonusing, and player tracking advanced fund transfer (AFT).
- ✓ Review physical payout forms for winners to make sure IT agents do not have access to process (e.g., create, approve, delete) payouts.

## 543.20(b)

As used in this section only, a system is any computerized system that is integral to the gaming environment. This includes, but is not limited to, the server and peripherals for Class II gaming system, accounting, surveillance, essential phone system, and door access and warning systems.

### Intent

Computerized 'systems' are defined as computerized systems integral to the operation of the gaming environment. Systems include electronic / electrical networked-system environments. The scope of computerized systems is not limited to just Class II player interfaces and Class II servers, but includes casino management systems (CMS), player tracking, accounting, door access, surveillance, and others.

### Testing

- ✓ Review the architectural plans, computerized network system design layout, and applications system inventory of the gaming operation to gain an understanding of the layout and scope of systems relating to Class II gaming that will be reviewed during an audit.
- ✓ Inquire with IT management and others to ensure a complete understanding of the operational layout and scope of systems to be assessed.

## 543.20(c)

Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;

### Intent

To ensure only authorized individuals can access computer systems, data, and networks both physically and logically, through networked applications and systems. This restricted access helps protect sensitive networks, programs, and data.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify controls in place for the control of both physical and logical access to the information technology environment used in conjunction with Class II gaming.
- ✓ Review user access lists and user group access lists to verify no unauthorized agents have access to the system under review.
- ✓ Verify that controls specified in the TICS, SICS, and IT policies and procedures for physical access to the IT environment have been implemented.

543.20(c)

Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(2) Physical and logical protection of storage media and its contents, including recovery procedures;

## Intent

To ensure that storage media and its contents are adequately protected both physically and logically, and that recovery procedures are in place to restore data in the event of a system failure.

## Testing

- ✓ Review TICS, SICS, and IT policies and procedures to determine if there are adequate physical data storage and data recovery controls and processes in place.
- ✓ Review data backup and recovery schedule to ensure it is completed at appropriate intervals defined in IT TICS and SICS pertaining to 543.20(j) Backup controls.
- ✓ Test and assess the physical data storage facility to ensure the facility is sufficient.
- ✓ Review additional physical protections of critical systems and storage media including, but not limited to, evaluations of door access systems, surveillance, fire suppression, HVAC systems, and logging personnel who enter and exit the area, to determine if they provide adequate protection.

543.20(c)

Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(3) Access credential control methods;

## Intent

To ensure only properly vetted and authorized personnel have access to the gaming operation’s secured logical and physical environments such as, key card systems, usernames and passwords, and physical keys and key control boxes.

## Testing

✓ Review TICS, SICS, and IT policies and procedures to ensure effective logical and physical access control methods are included.

✓ Review the user access list(s) and user group access list(s) (logical and physical) against the current employee and licensed vendor list(s).

✓ Review all critical systems that utilize access credential control methods including but not limited to, accounting and finance, casino management, player tracking, and key card systems.

## 543.20(c)

Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(4) Record keeping and audit processes; and

### Intent

To ensure that administrative bookkeeping and accurate and timely documentation supporting audit processes is maintained to uphold transparency and accountability in gaming operations and protect Tribal assets.

### Testing

- ✓ Review SICS to determine the controls the operation has established for record keeping and audit processes.
- ✓ Review previous internal and external audits to identify any findings regarding record keeping and audit processes and determine if they have been addressed.
- ✓ Review records kept by the IT operation (e.g., access logs related to various systems, log review and maintenance records) to verify records are maintained.

## 543.20(c)

Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(5) Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments.

### Intent

To ensure that technical departments and technical personnel are restricted from access to financial instruments including but not limited to, accounting, finance, payouts, and player bonusing systems. This provides accountability around conflicts of interest and protects Tribal assets.

### Testing

- ✓ Review TICS, SICS, and organizational chart(s) to identify employees who should have access to financial instruments.
- ✓ Review user and user group access permissions for systems impacting financial information as well as logs of access records (e.g., sign in log) to make sure they align with users' roles in the organizational charts. Flag accounts authorizing IT personnel to access financial instruments.

## 543.20(d): Physical security

(1) The information technology environment and infrastructure must be maintained in a secured physical location such that access is restricted to authorized agents only.

### Intent

To ensure that the information technology environment and supporting environments are maintained in a secure physical location to prevent unauthorized access with the goal of protecting against things such as theft, malware installation, data tampering, destruction and financial loss.

### Testing

✓ Conduct physical walkthrough inspection noting the access / denial methods to restrict physical access to critical locations (e.g., HID card, hard-key, biometrics, pin code, password, MFA).

## 543.20(d): Physical security

(2) Access devices to the systems' secured physical location, such as keys, cards, or fobs, must be controlled by an independent agent.

### Intent

To ensure that those who are recipients of the security access tools are not the same as those who authorize, manage, and assign security access tools to reduce the chance of dangers such as conflict of interest, insider threat and enhance accountability.

### Testing

- ✓ Review IT policies and procedures as well as the organizational chart(s) to verify roles, responsibilities, and organizational positions of the personnel responsible for physical access management.
- ✓ Note any potential independent conflicts and effectiveness of managerial oversight.
- ✓ In cases where staff headcount limits effectiveness, verify mitigating controls that reduce risks (e.g., independent access review processes and approval by multiple parties).

## 543.20(d): Physical security

(3) Access to the systems' secured physical location must be restricted to agents in accordance with established policies and procedures, which must include maintaining and updating a record of agents granted access privileges.

### Intent

To ensure only authorized agents, as specified by established policies and procedures, have access to physical locations. The policies and procedures must include keeping a current list of those agents who have access.

### Testing

- ✓ Review TICS, SICS, and policies and procedures to make sure a process is in place to authorize physical access to secure IT systems that include a log/record of agents with access.
- ✓ Review documentation or records of the approval process to verify established policies are followed.
- ✓ Review a random sample of access logs to secure IT locations and compare agents accessing the locations with the approved authorized user lists. Flag any access by unauthorized agents.

## 543.20(d): Physical security

(4) Network Communication Equipment must be physically secured from unauthorized access.

### Intent

To ensure the network infrastructure and equipment, organizational intranet, and all incoming and outgoing network communications are secured from unauthorized access.

### Testing

- ✓ Verify the Network Communication Equipment access control systems are physically secure from unauthorized access (i.e., the equipment is in a locked room or closet).
- ✓ Obtain network communications diagrams to include flow of internal and external data flows, hardware topology, and system application flows and review them to determine if the Network Communication Equipment is physically secured from unauthorized access.
- ✓ Perform a physical walkthrough of network communications architecture and facilities, including surveillance and security measures, looking for potential physical vulnerabilities (e.g., unlocked network closets and rack mounts, exposed network ports).

# 543.20(e): Logical security

(1) Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:

(i) Systems' software and application programs;

(ii) Data associated with Class II gaming; and

(iii) Communications facilities, systems, and information transmissions associated with Class II gaming systems.

## Intent

To ensure all organizational software systems as well as data and communication systems are restricted from unauthorized access.

## Testing

- ✓ Review TICS, SICS, and IT policies and procedures to make sure controls have been established to protect all systems by restricting and securing access to systems’ software and application programs; data associated with Class II gaming; and communications facilities, systems, and information transmissions associated with Class II gaming systems.
- ✓ Verify the effectiveness of security and operational controls supporting the physical and logical segregation of the organizational intranet and external internet connected systems. This can be accomplished by reviewing diagrams and technical documents along with any logs.
- ✓ Compare user and user group access lists against active employee lists and approved licensed vendor lists to ensure only authorized users have access to systems or application programs. NOTE: Discrepancies may be instances of noncompliance that should be addressed.

## 543.20(e): Logical security

(2) Unused services and non-essential ports must be disabled whenever possible.

### Intent

To ensure the deactivation or isolation of unused services (e.g., a service running on a server) and non-essential communication and computer ports (e.g., virtual IP ports, physical network jacks, and Wi-Fi access points).

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify they cover the processes of deactivation or isolation of unused services or ports.
- ✓ Conduct a walkthrough looking for open ports and access points in vacant offices, cubicles, conference rooms, and other accessible and restricted areas of the property.
- ✓ When/if accessible ports or access points are found, verify connectivity from that port or access point to gaming related networks.
- ✓ Request proof of firewall rules and VLAN segregation from network administrators. NOTE: If there are no rules or VLAN segregation.

## 543.20(e): Logical security

(3) Procedures must be implemented to ensure that all activity performed on systems is restricted and secured from unauthorized access, and logged.

### Intent

To ensure all actions taken on computer systems related to Class II gaming are properly recorded or logged, so there is a clear record of who did what and when.

### Testing

- ✓ Review SICS and IT policies and procedures to verify there are procedures in place to restrict and secure activity on Class II systems and that access is logged.
- ✓ Review logs of all actions taken on computer systems related to Class II gaming to ensure they contain appropriate detail for the system under review. The level of detail will vary from system to system.
- ✓ Observe how an action (e.g., steps, functions, commands) taken on a computer system related to Class II gaming is logged or recorded to verify the procedures are followed.
- ✓ Inquire with appropriate system administrator(s) to determine if processes and procedures are implemented to find and investigate discrepancies in logs of activity performed on systems.

## 543.20(e): Logical security

(4) Communications to and from systems via Network Communication Equipment must be logically secured from unauthorized access.

### Intent

To ensure that electronic communications to and from Class II gaming systems including, but not limited to, wireless, copper wire, satellite or cellular, is logically secured from unauthorized access.

### Testing

- ✓ Review TICS, SICS, and policies and procedures to verify a policy is in place that requires logical security measures protect Network Communication Equipment from unauthorized access.
- ✓ Conduct observations and inquire with IT agents responsible for network security control implementation to verify network security measures are in place to secure access to network systems including routers, firewalls, switches, virtual private networks (VPNs) or remote access systems, and Wi-Fi access points.
- ✓ Where applicable verify that encryption methods utilize adequate security. For example, check that wireless networks use current encryption standards (e.g., WPA2 or WPA3) and deprecated methods like WEP are not in use.
- ✓ Verify that software and firmware upgrades to communications equipment is current and controls are in place to ensure timely updates to software and firmware for relevant network communication equipment.

## 543.20(f): User controls

(1) Systems, including application software, must be secured with passwords or other means for authorizing access.

### Intent

To ensure that only authorized system account holders have access to computerized systems, including application software and other systems related to Class II gaming.

### Testing

- ✓ Verify that all critical accounting, financial, and other systems related to Class II gaming systems are secured with passwords or other means to limit logical system access.
- ✓ Review user access listings to verify unauthorized users do not have access to systems, including software, related to Class II gaming.

## 543.20(f): User controls

(2) Management personnel or agents independent of the department being controlled must assign and control access to system functions.

### Intent

To ensure only people who are not part of the department being monitored determine who gets access to certain system features. This separation helps prevent conflicts of interest and ensures proper oversight.

### Testing

- ✓ Review SICS to verify they include controls to adequately address agent independence with regards to the department or system requiring access controls.
- ✓ Review IT policies and procedures to make sure they include adequate processes to verify independent assignment and control access to system functions as well as processes to address personnel user access assignment or reassignment.
- ✓ Review user and user group access lists for discrepancies such as users with access to unauthorized and irrelevant system functions.
- ✓ In cases where managerial independence cannot exist due to limited staffing, verify there are mitigating controls to detect cases of unauthorized access and access rights being given (e.g., regular logging and access reviews).

(3) Access credentials such as passwords, PINs, or cards must be controlled as follows:

(i) Each user must have his or her own individual access credential;

(ii) Access credentials must be changed at an established interval approved by the TGRA; and

(iii) Access credential records must be maintained either manually or by systems that automatically record access changes and force access credential changes, including the following information for each user:

(A) User's name;

(B) Date the user was given access and/or password change; and

(C) Description of the access rights assigned to user.

## Intent

To ensure that all authorized access holders meet minimum credential requirements to retain their access permissions.

## Testing

- ✓ Review TICS, SICS, and group user account holders to verify they include the items specified in the MICS (see above) – there are no users with shared access credentials, access credentials are required to be changed periodically as established and approved by the TGRA, and access credential records are maintained.
- ✓ Review administrator-configured account parameter settings (e.g., password complexity, password reset interval) for group and individual user access settings. NOTE: For examples of current industry best practices regarding password complexity and schema, please reference the latest National Institute of Standards and Technology (NIST) guidelines.
- ✓ Look for and flag instances of shared accounts to access systems related to Class II gaming.

## 543.20(f): User controls

(4) Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by the TGRA.

### Intent

To ensure that lost or stolen user access credentials are deactivated within in the minimum time period stated by the TGRA, to prevent unauthorized access.

### Testing

- ✓ Review TICS, SICS, policies and procedures, and employee manuals to determine if employee and IT management actions and timelines for compromised access credentials are included.
- ✓ Review TICS, SICS, policies and procedures, and employee manuals to verify they establish specific timelines (i.e., avoid ‘ASAP’ and ‘immediately’) that are TGRA-approved for termination of user access credentials.
- ✓ If enough data for a data sample exists, verify that controls are being followed against examples of lost or compromised access credentials.

## 543.20(f): User controls

(5) Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.

### Intent

To ensure that the access credentials of terminated employees are quickly deactivated, within the time limit set by the TGRA, to prevent unauthorized access.

### Testing

- ✓ Review TICS, SICS, policies and procedures, and employee manuals to verify guidance for employees, IT Management, and Human Resources actions when employees are terminated are present.
- ✓ Review TICS, SICS, policies and procedures, and employee manuals to verify they establish specific timelines (i.e., avoid 'ASAP' and 'immediately') that are TGRA-approved for termination of user access credentials.
- ✓ Compare terminated employee list(s) to user access lists to determine if only active employees have access to systems.
- ✓ Review controls to verify procedures are in place that address access control management related to employee offboarding and changes in access right levels such as interdepartmental changes.
- ✓ Review controls in place to verify procedures are in place to manage access to systems when an employee leaves, voluntarily or involuntarily, or changes roles/teams/departments/business unit within the organization. NOTE: For examples of current best practices regarding timelines and processes for deactivating access credentials, please reference the latest NIST guidelines.

## 543.20(f): User controls

(6) Only authorized agents may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts.

### Intent

To ensure when any account, employee or patron, is inactive or closed, digital access must be restricted, and only individuals approved by the TGRA may access inactive or closed accounts.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures regarding user network security and access activity to verify measures that restrict access to inactive or closed accounts are in place.
- ✓ Verify appropriate access by comparing access logs/permissions to TICS/SICS/policies & procedures (e.g., patron player tracking accounts, employee user accounts).
- ✓ Compare access logs/permissions to TICS, SICS, and IT policies and procedures to verify access to inactive or closed accounts is only granted to authorized personnel.
- ✓ Review controls in place for access control management as related to employee offboarding and changes in access levels such as interdepartmental changes.

## 543.20(g): Installations and/or modifications

(1) Only TGRA authorized or approved systems and modifications may be installed.

### Intent

To ensure that organizational personnel must first seek approvals of TGRA and IT Management prior to the introduction of outside software or modifications to the network or computerized systems.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify the existence of a policy requiring TGRA authorization or approval for any Class II-related systems or modifications before they are installed.
- ✓ Test a sample of previous change management request forms for proper approvals and signatures to ensure the change management process is followed.
- ✓ Inquire with responsible agents to verify that all documentation for Class II and related systems is being recorded and maintained (e.g., Class II server file signature checks; Class II client file signature checks; independent test lab (ITL) such as GLI or BMM, certification letter; TGRA approval letter).
- ✓ Repeat review of change management request approvals and inquire with responsible agents as needed for other ITL certified systems, such as player tracking and/or casino management systems, and current version(s) of systems being implemented.

## 543.20(g): Installations and/or modifications

(2) Records must be kept of all new installations and/or modifications to Class II gaming systems. These records must include, at a minimum:

(i) The date of the installation or modification;

(ii) The nature of the installation or change such as new software, server repair, significant configuration modifications;

(iii) Evidence of verification that the installation or the modifications are approved; and

(iv) The identity of the agent(s) performing the installation/modification.

### Intent

To ensure detailed records are kept for new software installations, or any changes made to Class II gaming systems. The records must show what was done, when it was done, who did it, and proof that it was properly approved.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures regarding change management and asset management to verify the presence of a recordkeeping control for all new installations and/or modifications to Class II gaming systems.
- ✓ Test a random sample of records of each type for installations and / or modifications to Class II, Class III (when applicable), and casino management systems, such as a new pay table or version updated to an ITL-certified system to verify all required information was recorded.
- ✓ Inquire with responsible agents to verify that all documentation for Class II and related systems is being recorded and kept (e.g., Class II server signature check, Class II client signature check, ITL Certification letter, TGRA approval letter).
- ✓ Repeat records review and agent inquiries as needed for other ITL certified systems such as Player Tracking and/or Casino Management Systems.

543.20(g): Installations and/or modifications

(3) Documentation must be maintained, such as manuals and user guides, describing the systems in use and the operation, including hardware.

## Intent

To ensure current documentation, like manuals and user guides, is kept for all systems and equipment used in Class II gaming operations. This helps make sure IT agents understand how the systems work and supports troubleshooting, training, and audits.

## Testing

- ✓ Test a random sample of supporting system documentation, such as user manuals, specification sheets, and/or build sheets, to make sure the required documentation is kept or exists.
- ✓ Observe the locations where the sampled supporting system documentation is kept, verifying it is accessible. NOTE: Documentation may be stored or archived in an approved documentation storage file onsite, or on the vendor / manufacturer's website.

## 543.20(h): Remote access

(1) Agents may be granted remote access for system support, provided that each access session is documented and maintained at the place of authorization. The documentation must include:

(i) Name of agent authorizing the access;

(ii) Name of agent accessing the system;

(iii) Verification of the agent's authorization;

(iv) Reason for remote access;

(v) Description of work to be performed;

(vi) Date and time of start of end-user remote access session; and

(vii) Date and time of conclusion of end-user remote access session.

### Intent

To ensure remote access connections are secure, approved, and accurately recorded/logged.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify the controls for granting remote access require documentation that aligns with the MICS.
- ✓ Test a sample of remote access logs and verify that they contain at least the information listed in (i) through (vii). NOTE: Items (iv) and (v) cannot be a single record, they must be two items.
- ✓ Test the sample of remote access logs to verify that agents accessing systems (e.g., vendors) remotely have current licenses.

## 543.20(h): Remote access

(2) All remote access must be performed via a secured method.

### Intent

To ensure that all access to systems related to Class II gaming from outside the organization is performed in a secure method to minimize risks such as exposing sensitive data and systems to threats and breaches.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify a control requiring remote access via secure methods is present.
- ✓ Inquire with IT agents and have them describe the system used for remote access and explain how it is secure (e.g., encryption methods, authentication methods).
- ✓ Review supporting technical documentation of remote access-related systems for information regarding encryption methods and authentication methods to assess the security of the system. NOTE: Consider how the method compares to other methods and whether it is secure.

## 543.20(i): Incident monitoring and reporting

(1) Procedures must be implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.

### Intent

To ensure expedient and appropriate response to a variety of IT-related incidents, including but not limited to cybersecurity events, weather events, natural disasters, hardware failures, and software errors.

### Testing

✓ Review TICS, SICS, and IT policies and procedures to ensure procedures include proposed courses of action for each relevant incident type. Verify all procedures are up-to-date and approved by the TRGA.

✓ Review a random sample of incident response records, such as logs, investigation reports, and resolution documentation, to ensure incidents are properly tracked and resolved.

✓ Review that documented incidents were reported to the correct parties in the established time.

✓ Inquire with key personnel such as IT agents, security officers, and operation management to confirm they understand and follow the documented procedures (e.g., ask about recent incidents and how they were handled to assess real-world application).

✓ Verify that the facility has controls in place for monitoring such as intrusion detection systems and/or log management.

(2) All security incidents must be responded to within an established time period approved by the TGRA and formally documented.

## Intent

To ensure all IT security incidents are handled within a specific, practical time limit approved by the TGRA, and each incident response is recorded. These steps help make sure there is a quick and accountable response to IT security incidents to mitigate any risks.

## Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify they establish specific (i.e., avoid 'ASAP' and 'immediately') TGRA-approved response times for various types of IT-related security incidents.
- ✓ Review TICS, SICS, and IT policies and procedures to ensure they contain detailed controls regarding IT security incident documentation.
- ✓ Verify the TGRA has approved specific response times for various IT-related security incidents (e.g., TICS and/or SICS contain the same period specified in the policies and procedures or an email from the TGRA approving response times).
- ✓ Review a sample of recent incident reports to verify the response occurred within the approved timeframe, the incident was formally documented with sufficient detail.
- ✓ If incident report documentation is not sufficient, inquire with IT and Security agents to ensure they are aware of the TGRA-approved response timeframes and verify the control is being performed as intended. For example, ask how they determine the urgency of incidents and how they ensure timely responses.

## 543.20(j): Data backups

(1) Controls must include adequate backup, including, but not limited to, the following:

(i) Daily data backup of critical information technology systems;

(ii) Data backup of critical programs or the ability to reinstall the exact programs as needed;

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

(iv) Mirrored or redundant data source; and

(v) Redundant and/or backup hardware.

### Intent

To ensure that adequate data and software backup controls are in place to support expedient organizational data restoration of critical systems related to Class II gaming.

### Testing

- ✓ Review the TICS and SICS to verify that 'critical systems' such as financial, accounting, and player tracking, are defined.
- ✓ Review TICS, SICS, IT policies and procedures, and data backup schedules to confirm they include daily backups of critical systems, backup or reinstallation procedures for critical programs, secure storage of backup data, use of mirrored or redundant data sources, and the use of redundant and/or backup hardware.
- ✓ Verify both physically and logically secured storage of all backup data files and backup media. NOTE: this verification process will be different depending on the backup method(s) in use and may change periodically as technology changes.

## 543.20(j): Data backups

(2) Controls must include recovery procedures, including, but not limited to, the following:

(i) Data backup restoration;

(ii) Program restoration; and

(iii) Redundant or backup hardware restoration.

### Intent

To ensure gaming facilities have clear procedures for restoring data, software, and hardware related to Class II gaming to enable a quick recovery and resume operations after a system failure or disruption.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify they contain controls outlining system recovery processes including:
  - Data restoration steps. For example, the steps and programs the gaming operation will implement to retrieve a usable copy of the backup data.
  - Program reinstallation or restoration procedures. For example, the steps and programs the gaming operation will use to restore the operation's IT environment.
  - Hardware replacement or failover processes (e.g., mirrored systems, hot swap hardware, cold swap hardware, or failover service level agreement with a vendor).
- ✓ Review documentation for the applicable restoration and recovery systems and redundant hardware to determine if recovery procedures are safe and effective. NOTE: Documentation will vary depending on backup methodology and may change as technology changes.

543.20(j): Data backups

(3) Recovery procedures must be tested on a sample basis at specified intervals at least annually. Results must be documented.

## Intent

To ensure IT agents and management test the organization's recovery procedures and document the results at least once a year and determine if the recovery method works.

## Testing

- ✓ Review TICS, SICS and IT policies and procedures regarding recovery procedures to ensure testing of the procedures is required, at minimum, every year.
- ✓ Review the last completed annual recovery testing documentation including, a record of test performed and validity of data after recovery to ensure the data is usable.
- ✓ Inquire with IT agents to determine knowledge of testing procedures, timelines, recordkeeping, and reporting processes.

## 543.20(j): Data backups

(4) 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.

### Intent

To ensure backup data files and recovery components are protected just as securely as the original systems they support, to prevent unauthorized access and protect Tribal assets.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify they include controls requiring backup data files and recovery components are managed with at least the same level of security and access control as the system they support.
- ✓ Inquire with IT agents to assess whether operational controls are followed. Compare responses to written documentation (e.g., SIGC, procedures) to identify possible inconsistencies in security across systems.
- ✓ Review user and user group access lists, access validation methods, and supporting documentation regarding the security of the data backup system(s) in use and look for inconsistencies in level of security and access controls. NOTE: All systems related to data backups should be reviewed.
- ✓ Verify that security for backup data files and recovery components is adequate and equal to the systems they support (e.g., Look for cases of inadequate passwords, encryption, physical security, and/or user controls).
- ✓ Verify both physically and logically secured storage of all backup data files and backup media. NOTE: this verification process will be different depending on the backup method(s) in use and may change periodically as technology changes.

## 543.20(k): Software downloads

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

### Intent

To ensure any downloads to Class II gaming systems, whether done automatically or manually, follow strict federal standards, as outlined in 25 CFR § 547.12, and are secure, accurate, and do not disrupt gaming operations.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify that controls are in place outlining the process of downloading software for Class II gaming systems and their respective signature verification processes.
- ✓ Evaluate TICS, SICS and IT policies and procedures to ensure they are adequate and comply with all parts of 25 CFR § 547.12.
- ✓ Inquire with IT agents to verify software downloads are delivered through secure methods and follow documented policies and procedures.
- ✓ Test a random sample of automatically downloaded Class II system (e.g., Class II server, Class II pay tables, and player tracking) records to verify that the Class II system has recorded at least the (a) date and time of the initiation, (b) completion of any download, (c) the components that received it, (d) the version of the download package and any software downloaded, (e) status of the download attempt (i.e., success or failure), and (f) unique identifier of individual conducting or scheduling the download.
- ✓ Test a sample of completed downloads to verify the signature verification is complete, recorded, and meets the requirements specified in the ITL certification letter.

## 543.20(l): Verifying downloads

Following download of any Class II gaming system software, the Class II gaming system must verify the downloaded software using a software signature verification method. Using any method it deems appropriate, the TGRA must confirm the verification.

### Intent

To ensure that following the download of Class II gaming system software, the gaming system must verify the download with a software signature verification method to confirm files are not corrupted, tampered with, or missing.

### Testing

- ✓ Review TICS, SICS, and IT policies and procedures to verify the software download method is adequate to prevent an invalid software file signature check.
- ✓ Verify software download method has been approved by the TGRA.
- ✓ Test records to confirm TGRA approval of software and TGRA verification of signature checks, ITL certification letters, and the approval process.