Local Agency Security Officer

LASO HANDBOOK

National Indian Gaming Commission

Version 5.9.4
04/26/2024

Preamble:

The NIGC CJIS Audit Unit (CAU) hopes you will use this Local Agency Security Officer (LASO) Handbook as an aid to assist in the development of your own policy and procedures. This handbook is a tool and not meant to be duplicated word for word but is intended to guide the LASO and staff to understand the responsibilities of being an authorized recipient of Federal Bureau of Investigation (FBI) Criminal History Record Information (CHRI). Please utilize this tool to develop your own policies and procedures according to your specific practices and systems.

The CAU team is available to assist you and your team at your request.

Visit the NIGC CJIS Resource Page for more information.

Table of Contents

Initial Steps to CJIS Compliance

1) Review the NIGC 2021 CHRI Memorandum of Understanding (MOU).
    a. Ensure all authorized personnel have reviewed the MOU.
2) Review the NIGC CJIS Resource Materials.
3) Designate Local Agency Security Officer (LASO) and notify iso@nigc.gov.
4) Develop and maintain an Authorized Personnel List (APL).
    a. List all personnel with access to FBI Criminal History Record Information (CHRI) received from NIGC, and
    b. Send the APL to NIGC Information Security Officer (ISO) at iso@nigc.gov.
    c. Maintain an up-to-date APL on site and on record with the NIGC ISO.
    d. Maintain up to date Tribal Management Services (TMS) Portal user access.
5) Provide and document initial security and privacy literacy training to all new system users per CJIS Security Policy (CJISSECPOL) Version 5.9.4, Policy Area 5.2.
    a. At the discretion of the LASO, satisfy this requirement by obtaining initial security and privacy literacy training at CJIS Online.
6) Develop/refine written internal TGRA policies to meet CJISSECPOL requirements.
    a. Policy Area 1—Information Exchange Agreements
    b. Policy Area 2—Awareness and Training (AT)
    c. Policy Area 3—Incident Response (IR)
    d. Policy Area 4—Auditing and Accountability (AU)
    e. Policy Area 5—Access Control (AC)
    f. Policy Area 6—Identification and Authentication (IA)
    g. Policy Area 7—Configuration Management
    h. Policy Area 8—Media Protection (MP)
    i. Policy Area 9—Physical and Environmental Protection (PE)
    j. Policy Area 10—Systems and Communications Protection (SC)
    k. Policy Area 11—Formal Audits
    l. Policy Area 12—Personnel Security
    m. Policy Area 13—Mobile Devices
    n. Policy Area 14—System and Services Acquisition (SA)
    o. Policy Area 15—System and Information Integrity (SI)
    p. Policy Area 16—Maintenance (MA)
    q. Policy Area 17- Planning (PL)
    r. Policy Area 18—Contingency Planning (CP)
    s. Policy Area 19—Risk Assessment (RA)
7) Complete and document internal training on TGRA policies.
8) Complete and document authorized personnel training and Personnel Sanctions of Standards Discipline Form for TGRA policies.
9) Determine if a contractor performs noncriminal justice administrative functions with access to FBI CHRI. If so, the TGRA/Tribe must request and receive written permission from the FBI Compact Officer. (Refer to NIGC CJIS Resource Materials **"Outsourcing Agreement Resources."**)
10) Establish regular internal auditing/monitoring to maintain compliance with FBI requirements.
11) Monitor and ensure annual training for users and for outsourced non-channelers.

LASO Policy and Procedure

I. PURPOSE OF THIS SECTION

A. This section outlines the responsibilities of the Tribe's designated Local Agency Security Officer (LASO). Per the FBI CJIS Security Policy (CJISSECPOL) Section 3.2.9.[1]

II. ACTIONS

A. Each Tribe with an executed NIGC 2021 CHRI Memorandum of Understanding (MOU) shall designate a LASO. The Tribe or TGRA shall ensure that if the TGRAs LASO changes, the new LASO will review a copy of the MOU within ten (10) business days of assuming the position as well as notify the NIGC Information Security Officer (ISO) (iso@nigc.gov) of their name and contact information within that timeframe.

B. The LASO acts as the primary liaison between the Tribe or TGRA and is responsible for coordinating Tribal compliance with all regulations pertaining to the access, use, handling, dissemination, and destruction of Criminal Justice Information (CJI) and CHRI. The LASO should ensure they are aware of all areas in which CHRI is maintained, digitally or non-digitally, and ensure that policy areas reflect the Tribe's processes, and procedures protect CHRI and maintain its security. The LASO should review Appendix A, and NIGC Bulletin No.2022-3 Criminal History Record Information (CHRI) Retention to aid with achieving CHRI compliance.

C. The LASOs responsibilities include but are not limited to:
   1. Utilizing the Noncriminal Justice Agency Information Change Form for notifying the NIGC ISO:
      a. Within ten (10) days of appointing a new LASO.
      b. Authorized Tribal signatory changes.
      c. Any other relevant business information: such as, Tribal name change, mailing or physical address, and/or main telephone number changes.
   2. Developing and maintaining an Authorized Personnel List (APL)[2] to identify who is using the approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same. The LASO will send the APL and any changes to it to the NIGC ISO as changes occur (Refer to Part A. Authorized Personnel).
      a. Ensuring the users added to the Tribal Management Services (TMS) Portal are authorized to access CHRI and have completed appropriate training. (Refer to Appendix C)
      b. Removing users from the Tribal Management Services (TMS) Portal that no longer require access to CHRI. (Refer to Appendix D)
   3. Develop and maintain a network diagram to identify and document how the equipment is connected to the system (Refer to Part B. Network Diagram Development).

[1] Each LASO shall: 1. Create an APL. 2. Create and maintain a network diagram. 3. Ensure awareness and training completion. 4. Develop policy and procedures and audit to ensure they are working. 5. Create incident response policy.

[2] CJISSECPOL 5.9.1.2 Physical Access Authorizations: The Tribe or TGRA shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

4. Maintain and ensure awareness and training for personnel security screening procedures, ensuring they are being followed as stated in the Awareness and Training Policy (Refer to Part C. Awareness and Training Policy).
5. Ensure there are developed policies, procedures, and audits to ensure the approved and appropriate security measures are in place and working as expected (Refer to Part D. Auditing and Accountability).
6. Ensure there is an incident reporting policy and required notifications of security incidents are promptly transmitted (Refer to Part E. Incident Response).

D. The LASOs responsibilities during an NIGC audit include the following:
   1. Ensuring all audit instructions are followed and that the audit packet is returned to the NIGC CJIS Audit Unit in a timely manner.
   2. Being present for the audit interview and notifying/gathering any other Tribe/Authorized personnel who may be needed to answer the auditor's questions.
   3. Having all requested documentation available for the audit.
   4. Serving as the primary coordinator for any corrective actions stemming from the audit findings.

E. The LASO ensures monthly audits are conducted to verify each fingerprint submission is for the specific purpose of Key Employee and/or Primary Management Official licensing pursuant to IGRA and NIGC regulations.
   1. Per 2021 CHRI MOU V.B.13- The Tribe/TGRA will notify the NIGC, on a monthly basis, of the following licensing information associated with the dissemination of CHRI for a fingerprinted applicant that does not result in a submission of a NOR:
      a. The reason for the fingerprint submission, and;
      b. If the submission was in error, the steps taken to correct the process that created the error.

F. Prior to engaging in outsourcing any noncriminal justice administrative functions with a Contractor, the LASO will review the Outsourcing Agreement Resources available at NIGC CJIS Resource Materials and utilize the sample documents to request and receive written permission from the FBI Compact Officer per the Security and Management Control Outsourcing Standard for Non-Channelers.
   1. The LASO shall provide written notice of any early voluntary termination of contract to the FBI Compact Officer.

G. Per CJISSECPOL 5.12.4 the LASO will ensure to employ a formal sanctions process for personnel failing to comply with established security policies and procedures.

H. The LASO will update policies annually, when security incidents occur; or when changes are made to the FBI CJIS Security Policy.

Part A. Authorized Personnel

I. PURPOSE OF THIS SECTION

Per CJISSECPOL 5.9.1.2 Physical Access Authorizations: The Tribe shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

A. Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing, and transmission of CJI/CHRI and the modification of information systems, applications, services, and communication configurations allowing access to CJI/CHRI. Per the CJISSECPOL 5.5.1, the Tribe or TGRA shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts and validate information system accounts at least annually, documenting the validation process.

II. ACTIONS

A. The Tribe or TGRA will approve individual access privileges; and will enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency will enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The Tribe will implement the least privilege, based on specific duties, operations, or information systems, as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know. The LASO will develop an Authorized Personnel List (APL) and submit to the iso@nigc.gov. Any changes to the APL require a completely new submission of the revised APL to iso@nigc.gov.

B. The LASO will develop procedures to:
   1. Manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.
   2. Validate information system accounts at least annually and document the validation process.
   3. Identify authorized users of the information system and specify access rights/privileges.
   4. Grant access to the information system based on:
      a. Valid need-to-know/need-to-share that is determined by assigned official duties.
      b. Satisfaction of all personnel security criteria.

C. The LASO will ensure the following:
   1. The person(s) responsible for account creation will be notified when:
      a. A user's information system usage or need-to know or need-to-share changes.
      b. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

D. The information system will:
   1. Enforce assigned authorizations for controlling access to the system and contained information.
   2. Restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.[3]

E. The LASO will:
   1. Employ access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.
   2. Approve individual access privileges and enforce physical and logical access restrictions associated with changes to the information system and generate, retain, and review records reflecting all such changes.
   3. Enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.
   4. Implement least privilege, based on specific duties, operations, or information systems, as necessary to mitigate risk to CJI.[4]
   5. Maintain the logs of access privilege changes for a minimum of one year or at least equal to the Tribe/TGRAs record retention policy - whichever is greater.
   6. Restrict by object (e.g., data set, volumes, files, records), including the ability to read, write, or delete the objects, the access control mechanisms to enable access to CJI.

F. The LASO will ensure:
   1. The access controls in place and operational for all IT systems will:
      a. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the Tribe/TGRA grants authority based upon operational business needs.
      b. Document the parameters of the operational business needs for multiple concurrent active sessions.
      c. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

G. The LASO will control access to CJI based on one or more of the following:
   1. Job assignment or function (i.e., the role) of the user seeking access.
   2. Physical location.
   3. Logical location.
   4. Network addresses (e.g., users from sites within a given Tribe/TGRA may be permitted greater access than those from outside).
   5. Time-of-day and day-of-week/month restrictions.

[3] Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).
[4] This limits access to CJI to only authorized personnel with the need and the right to know.

H. The LASO will use one or more of the following mechanisms when setting up access controls:
   1. Access Control Lists (ACLs).[5]
   2. Resource Restrictions.[6]
   3. Encryption.[7]
   4. Application Level.[8]

I. The LASO will ensure policy requirements as follows:
   1. The system enforces a limit of no more than five (5) consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI).
   2. The system automatically locks the account/node for a 10-minute period unless released by an administrator.

J. The LASO will ensure the information system:
   1. Displays an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules.
   2. Uses notification message, which at a minimum, provides the following information:
      a. The user is accessing a restricted information system.
      b. System usage may be monitored, recorded, and subject to audit.
      c. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
      d. Use of the system indicates consent to monitoring and recording.

K. The LASO will ensure the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

L. Privacy and security policies will be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance.

M. System use notification messages will be implemented in the form of warning banners displayed when individuals log in to the information system.

---

[5] ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
[6] Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.
[7] Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in CSP 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
[8] In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

N. For publicly accessible systems:
   1. The system use information is available and when appropriate, is displayed before granting access.
   2. Any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities.
   3. The notice given to public users of the information system includes a description of the authorized uses of the system.

O. The LASO will ensure the information system prevents further access to the system by initiating a session lock[9] after a maximum of 30 minutes of inactivity.

P. The session lock (screen saver with a password) will remain in effect until the user re-establishes access using appropriate identification and authentication procedures.

Q. The users will directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.

R. The LASO will ensure the TGRAs:
   1. Authorize, monitor, and control all methods of remote access to the information system.
   2. Employ automated mechanisms to facilitate the monitoring and control of remote access[10] methods.
   3. Control all remote accesses through managed access control points.
   4. Permit remote access for privileged functions only for compelling operational needs but document the technical and administrative process for enabling remote access to the information system for privileged functions in the security plan.

S. Virtual escorting of privileged functions will be permitted only when all the following conditions are met:
   1. The session will always be monitored by an authorized escort.
   2. The escort will be familiar with the system/area in which the work is being performed.
   3. The escort will have the ability to end the session at any time.
   4. The remote administrative personnel connection will be via an encrypted (FIPS 140-2 certified) path.
   5. The remote administrative personnel will be identified prior to access and authenticated prior to or during the session.[11]

T. The Tribe or TGRA will NOT allow publicly accessible computers[12] to be used to access, process, store, or transmit CJI.

---

[9] A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation are exempt from this requirement.
[10] Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).
[11] This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.
[12] Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

III. SELF-AUDIT

a. Sample Audit Checklist for CJISSECPOL Policy Area 5 Access Control.

Part B. Network Diagram Development

I. PURPOSE OF THIS SECTION

A. CJISSECPOL 5.7.1.2 Network Diagram. The Tribe or TGRA shall ensure that a complete topological drawing depicting the interconnectivity of the agency network to criminal justice information, systems, and services is maintained in a current status (Refer to Appendix E).

II. ACTIONS

A. Per the CJISSECPOL, the LASO will ensure the network topological drawing will include:
   1. All communications paths, circuits, and other components are used for the interconnection, beginning with the Tribe/TGRA-owned system(s) and traversing through all interconnected systems to the endpoint.
   2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations do not have to be shown; the number of clients is sufficient.
   3. "For Official Use Only" (FOUO) markings.
   4. The agency name and date (day, month, and year) drawing were created or updated.
   5. The LASO will protect the system documentation from unauthorized access consistent with the provisions described in CJISSECPOL Policy Area 5.5 Access Control.

III. SELF-AUDIT

A. The sample Audit Checklist for CJISSECPOL Policy Area 7 Configuration Management.

Part C. Awareness and Training Policy

I. PURPOSE OF THIS SECTION

A. The Tribe or TGRA shall provide role-based security and privacy training to personnel. Per CJISSECPOL Awareness Training (AT), AT-3 Role Based Training.
   1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and
   2. When required by system changes.

II. ACTIONS

A. The Tribe or TGRA shall develop an organizational-level awareness and training policy to ensure all personnel with physical or logical access[13] to CJI[14]/ CHRI[15] are aware of their specific individual responsibilities and expected behavior when they access it or systems that contain or process it.

B. The LASO will ensure authorized personnel are enrolled, assigned, and complete AT through the NIGC provided Peak Performance's CJIS Online or equivalent training from another source.

C. In lieu of utilizing CJIS Online, the LASO will do the following:
   1. Develop, document, and disseminate its organization-level awareness and training policy to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CHRI.
   2. Develop an organization-level awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls.
   3. Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy and procedures.
   4. Review and update the current awareness and training policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJISSECPOL are made.

---

[13] The physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI.

[14] Criminal Justice Information (CJI) is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

[15] Criminal History Record Information (CHRI) is a subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information, or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

5. Review and update procedures annually and following changes in information system operating environment, when security incidents occur, or when changes in the CJISSECPOL are made.
6. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors) as part of initial training for new users prior to their accessing CJI and annually thereafter.
7. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors) when required by system changes or within 30 days of any security event for individuals involved in the event.

D. The LASO will employ one or more of the following techniques to increase the security and privacy awareness of system users:
   1. Displaying posters.
   2. Offering supplies inscribed with security and privacy reminders.
   3. Displaying logon screen messages.
   4. Generating email advisories or notices from organizational officials.
   5. Conducting awareness events.

E. The LASO will:
   1. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJISSECPOL.
   2. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.
   3. Provide literacy training on recognizing and reporting potential indicators of insider threats.
   4. Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

F. The LASO will provide role-based security and privacy training to personnel with the following roles and responsibilities:
   1. All individuals with unescorted access to a physically secure location.
   2. General User.[16]
   3. Privileged User.[17]
   4. Organizational Personnel with Security Responsibilities.[18]

G. The LASO will:
   1. Provide role-based security and privacy training to personnel before authorizing access to the system, information, or performing assigned duties, and annually thereafter.
   2. Provide role-based security and privacy training to personnel when required by system changes.

[16] A user, but not a process, who is authorized to use an information system.
[17] A user that is authorized (and, therefore, trusted) to perform security relevant functions that general users are not authorized to perform.
[18] Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.

3. Update role-based training content annually and following audits; changes in the information system operating environment; security incidents; or when changes are made to the CJISSECPOL.
4. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.
5. Incorporate the minimum following topics into appropriate role-based training content for all individuals with unescorted access to a physically secure location.
6. Adhere to all CJISSECPOL Awareness and Training guidance and may utilize Peak Performance CJIS Online training for LASOs and all authorized users.

H. The LASO will provide all personnel with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI.

I. The LASO will document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training.

J. The LASO will retain individual training records for a minimum of three years.

III. SELF-AUDIT

A. The Sample Audit Checklist for CJISSECPOL Policy Area 2 Awareness Training.

Part D. Auditing and Accountability

I. PURPOSE OF THIS SECTION

A. Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and are not necessarily applied to every user level workstation within the Tribe or TGRA. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

II. POLICY

A. The LASO will:
   1. Develop, document, and disseminate to organizational personnel with audit and accountability responsibilities an agency and system-level audit and accountability policy that:
      a. Address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
   2. Develop procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls.
   3. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability policy and procedures.
   4. Review and update the current audit and accountability:
      a. Policy annually and following any security incidents involving unauthorized access to Criminal Justice Information (CJI) or Criminal Justice History Record Information (CHRI) or systems used to process, store, or transmit CJI/CHRI.
      b. Procedures annually and following any security incidents involving unauthorized access to CJI/CHRI or systems used to process, store, or transmit CJI/CHRI.
   5. Identify the types of events that the system is capable of logging in support of the audit function (e.g., authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions).
   6. Coordinate the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged.

B. The LASO will ensure the following events are logged:
   1. Successful and unsuccessful system log-on attempt.
   2. Successful and unsuccessful attempts to use:
      a. Access permission on a user account, file, directory, or other system resource.
      b. Create permission on a user account, file, directory, or other system resource.
      c. Write permission on a user account, file, directory, or other system resource.
      d. Delete permission on a user account, file, directory, or other system resource.

e. Change permission on a user account, file, directory, or other system resource.
f. Access permission on a user account, file, directory, or other system resource.
g. Successful and unsuccessful attempts to change account passwords.

C. Successful and unsuccessful actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.).
   1. Successful and unsuccessful attempts for users to:
      (1) Access the audit log file.
      (2) Modify the audit log file.
      (3) Destroy the audit log file.

D. The LASO will:
   1. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.
   2. Review and update the event types selected for logging annually.

E. The LASO will ensure that audit records contain information that establishes the following:
   1. What type of event occurred.
   2. When the event occurred.
   3. Where the event occurred.
   4. Source of the event.
   5. Outcome of the event.
   6. Identity of any individuals, subjects, or objects/entities associated with the event.

F. The LASO will generate audit records containing the following information:
   1. Session, connection, transaction, and activity duration.
   2. Source and destination addresses.
   3. Object or filename involved.
   4. Number of bytes received, and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.

G. The LASO will limit personally identifiable information (PII) contained in audit records to the following elements identified in the privacy risk assessment:
   1. Minimum PII necessary to achieve the purpose for which it is collected (Refer to CJISSECPOL Section 4.3).

H. The LASO will:
   1. Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements.
   2. Alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure.
   3. Will take additional actions and restart all audit logging processes and verify system(s) are logging properly.

I. The LASO will:
   1. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.
   2. Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities.
   3. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
   4. Integrate audit record review, analysis, and reporting processes using automated mechanisms.
   5. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

J. The LASO shall provide and implement an audit record reduction and report generation capability that:
   1. Supports on-demand audit record review, analysis, and reporting requirements and after- the-fact investigations of incidents, and
   2. Does not alter the original content or time ordering of audit records.

K. The LASO shall provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: information included in
AU-3.[19]

L. The LASO will ensure that internal system clocks are used to generate time stamps for audit records and ensure to record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

M. The LASO will ensure protection of audit information and audit logging tools from unauthorized access, modification, and deletion.

N. The LASO shall alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.

[19] Please refer to questions #10-12 of the CJISSECPOL Policy Area 4 Audit and Accountability sample audit checklist.

O. The LASO will authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators.
   1. The Tribe or TGRA will:
      a. Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.
      b. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a[20] on all systems generating required audit logs.
      c. Allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system.
      d. Generate audit records for the event types defined in AU-2c[21] that include the audit record content defined in AU-3.[22]

III. SELF-AUDIT

A. The Sample Audit Checklist for CJISSECPOL Policy Area 4 Audit and Accountability.

[20] Please refer to question #5 of the CJISSECPOL Policy Area 4 Audit and Accountability sample audit checklist.
[21] Please refer to question #7 of the CJISSECPOL Policy Area 4 Audit and Accountability sample audit checklist.
[22] Please refer to questions #10-12 of the CJISSECPOL Policy Area 4 Audit and Accountability sample audit checklist.

Part E. Incident Response

I. PURPOSE OF THIS SECTION

A. 2021 CHRI MOU- Guidance Appendix: CJISSECPOL – summary of primary requirements– In the MOU, the TGRA agreed to comply with the FBI CJISSECPOL.
   1. The TGRA shall create and keep current an Incident Handling policy, in accordance with CJISSECPOL 5.3, which outlines response procedures for all security incidents relating to CJI/CHRI and the system(s) used to access, store, and transmit them. This policy must include incidents involving employees, contractors, and third-party users.
   2. The procedures shall include incident handling capability for security incidents: preparation, detection and analysis, containment, eradication, and recovery as well as tracking and documenting each incident, including user response activities.
   3. Within six (6) months of executing the NIGC MOU, the LASO shall implement the Incident Handling procedures, reporting incidents to the NIGC ISO (iso@nigc.gov), Security Incident Response Form.
   4. Initial reports of security incidents shall be made to the NIGC ISO (iso@nigc.gov)within 24 hours of detection.

II. POLICY

A. The Tribe and or TGRA shall develop, document, and disseminate an incident response policy and procedures to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI.

B. The Tribe and or TGRA shall have an agency-level incident response policy that:
   1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
   2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

C. The Tribe shall have procedures to facilitate the implementation of the incident response policy and the associated incident response controls.

D. The Tribe shall designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures.

E. The LASO shall review and update the current incident response:
   1. Policy annually and following any security incidents involving unauthorized access to Criminal Justice Information (CJI) or Criminal Justice History Record Information (CHRI) or systems used to process, store, or transmit CJI/CHRI.
   2. Procedures annually and following any security incidents involving unauthorized access to CJI/CHRI or systems used to process, store, or transmit CJI/CHRI.

F. The LASO shall provide incident response training to system users consistent with assigned roles and responsibilities:
   1. Prior to assuming an incident response role or responsibility or acquiring system access.
   2. When required by system changes.
   3. Annually thereafter.

G. The LASO shall:
   1. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI/CHRI or systems used to process, store, or transmit CJI/CHRI.
   2. Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.
   3. Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests.
   4. Coordinate incident response testing with organizational elements responsible for related plans.

H. The LASO shall:
   1. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.
   2. Coordinate incident handling activities with contingency planning activities.
   3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly?
   4. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

I. The Tribe or TGRA shall support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.)

J. The LASO shall track and document incidents.

K. The LASO shall:
   1. Require personnel to report suspected incidents to the organizational incident response capability immediately but not to exceed one (1) hour after discovery.
   2. Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the NIGC Information Security Officer (ISO) and FBI CJIS Division ISO.

L. The Tribe or TGRA shall report incidents using automated mechanisms.

M. The Tribe or TGRA shall provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

N. The LASO shall provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

O. The LASO shall increase the availability of incident response information and support using automated mechanisms that provide a push or pull capability for users to obtain incident response assistance. (For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.)

P. The LASO shall develop an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability.
   2. Describes the structure and organization of the incident response capability.
   3. Provides a high-level approach for how the incident response capability fits into the overall organization.
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions.
   5. Defines reportable incidents.
   6. Provides metrics for measuring the incident response capability within the organization.
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability.
   8. Addresses the sharing of incident information.
   9. Is reviewed and approved by the organization's/agency's executive leadership annually.
   10. Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities.

Q. The LASO shall:
   1. Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities.
   2. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
   3. Communicate incident response plan changes to organizational personnel with incident handling responsibilities.
   4. Protect the incident response plan from unauthorized disclosure and modification.

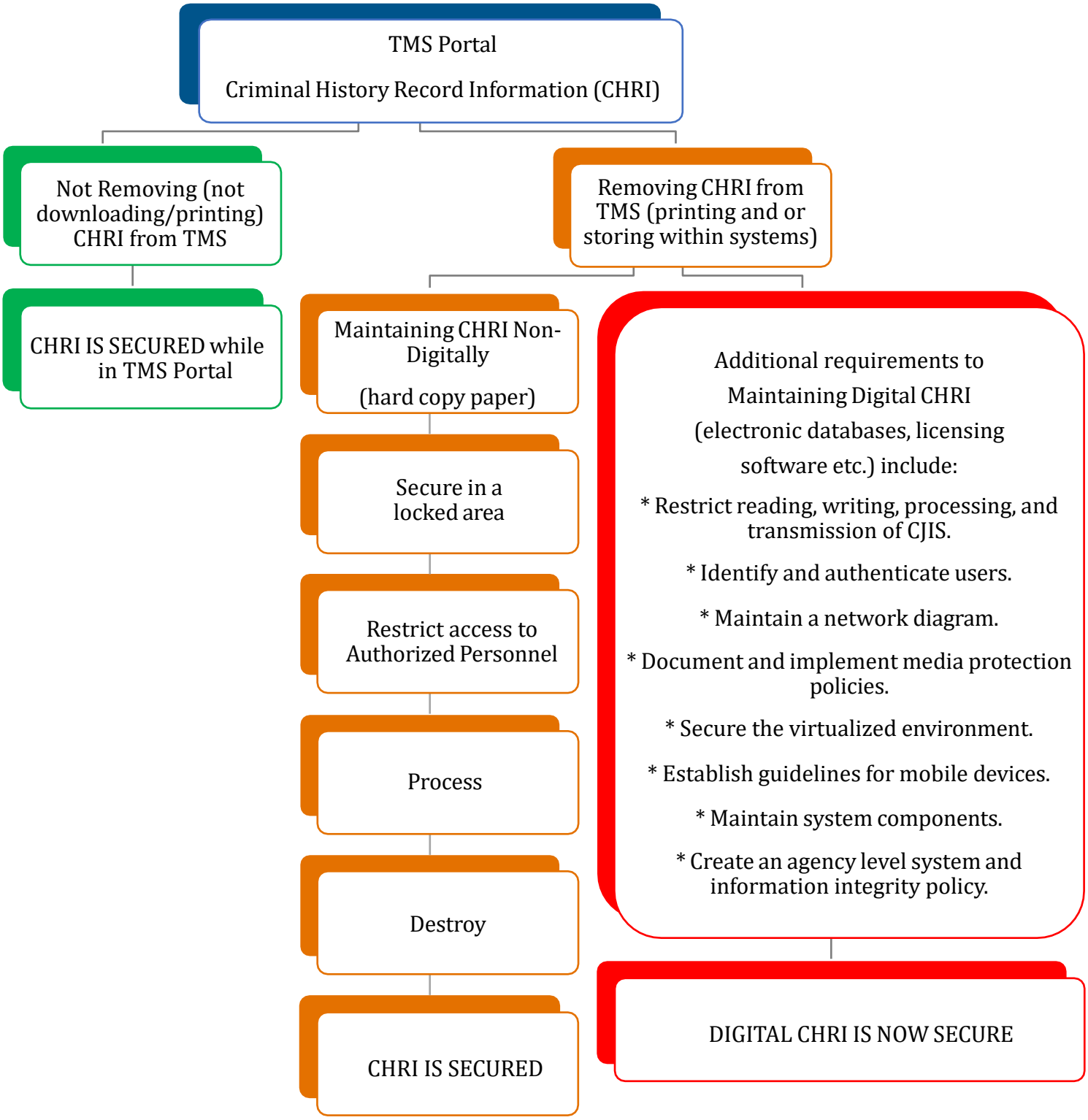
R. The Tribe or TGRA shall include the following in the Incident Response Plan for breaches involving personally identifiable information:
   1. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed.
   2. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms.
   3. Identification of applicable privacy requirements.

III. SELF-AUDIT

A. The Sample Audit Checklist for CJISSECPOL Policy Area 3 Incident Response.

Appendices

Appendix A- CHRI Storage



Appendix B- Sample Audit Checklists for CHRI Storage

"Get to Green" Checklists for compliance:

- Sample Audit Checklist Information Exchange Agreements
- Sample Audit Checklist Awareness and Training (AT)
- Sample Audit Checklist Incident Response (IR)
- Sample Audit Checklist Media Protection (MP)
- Sample Audit Checklist Physical and Environmental Protection (PE)
- Sample Audit Checklist Personnel Security

"Orange Caution" Checklists for compliance:

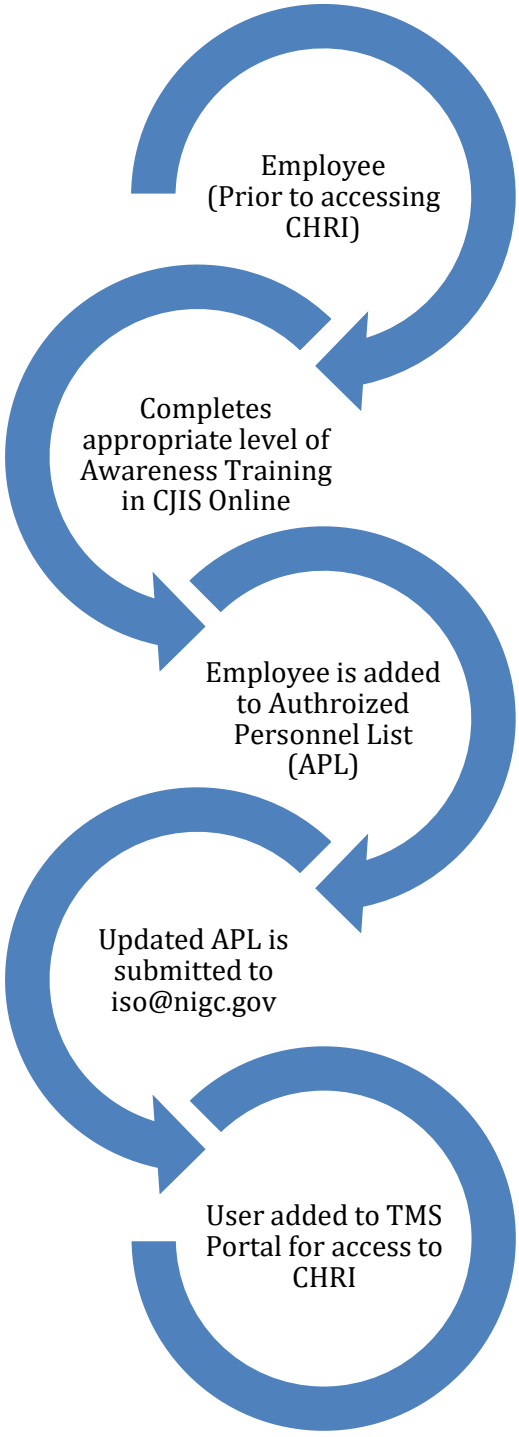
- Sample Audit Checklist Information Exchange Agreements
- Sample Audit Checklist Awareness and Training (AT)
- Sample Audit Checklist Incident Response (IR)
- Sample Audit Checklist Media Protection (MP)
- Sample Audit Checklist Physical and Environmental Protection (PE)
- Sample Audit Checklist Personnel Security
- Sample Audit Checklist Access Control (AC)

"Red Aware" Checklists for compliance:

- Sample Audit Checklist Information Exchange Agreements
- Sample Audit Checklist Awareness and Training (AT)
- Sample Audit Checklist Incident Response (IR)
- Sample Audit Checklist Auditing and Accountability (AU)
- Sample Audit Checklist Access Control (AC)
- Sample Audit Checklist Identification and Authentication (IA)
- Sample Audit Checklist Configuration Management
- Sample Audit Checklist Media Protection (MP)
- Sample Audit Checklist Physical and Environmental Protection (PE)
- Sample Audit Checklist Systems and Communications Protection (SC)
- Sample Audit Checklist Personnel Security
- Sample Audit Checklist Mobile Devices
- Sample Audit Checklist System and Services Acquisitions (SA)
- Sample Audit Checklist System and Information Integrity (SI)
- Sample Audit Checklist Maintenance (MA)
- Sample Audit Checklist Planning (PL)
- Sample Audit Checklist Contingency Planning (CP)
- Sample Audit Checklist Risk Assessment (RA)

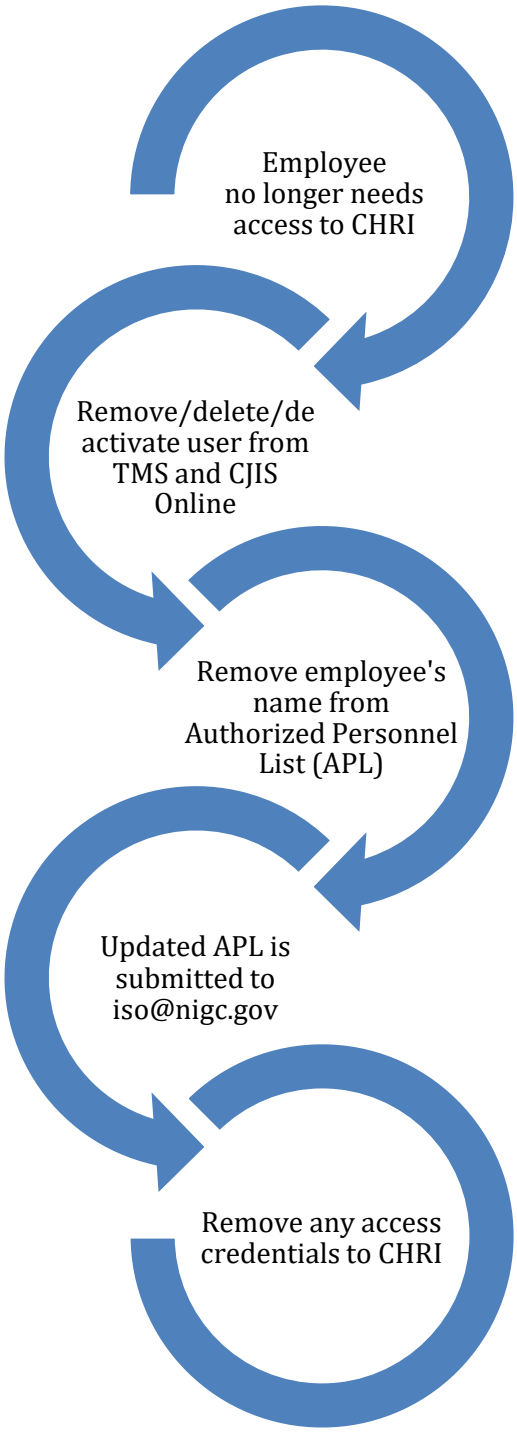
Appendix C- Authorizing Access to CHRI

Prior to adding users to Tribal Management Services (TMS) Portal and authorizing access to CHRI, the LASO shall ensure the individual has received appropriate training and appears on the Authorized Personnel List submitted to iso@nigc.gov.



Appendix D- Removing Access to CHRI

When a user or employee no longer needs access to Tribal Management Services (TMS) Portal. The LASO will remove user access to CHRI in the Tribal Management Services (TMS) Portal and remove name from the APL.



Appendix E- Network Diagram SAMPLE

Network diagrams are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the "big picture" – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the way each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.