Local Agency Security Officer

LASO HANDBOOK

National Indian Gaming Commission

Version 5.9.2
11/01/23

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 Service (TMS) user access.
5) Provide and document initial security and privacy literacy training to all new system users per CJIS Security Policy (CJISSECPOL) Version 5.9.3, 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
    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 Protection
    j. Policy Area 10—Systems and Communications Protection
    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)
7) Complete and document internal training on TGRA policies.
8) Complete and document authorized personnel training/penalty acknowledgment statements 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. (Please see 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 B, to aid with determining 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) 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).
3. Develop and maintain a network diagram to identify and document how the equipment is connected to the system (Refer to Part B).
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).
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).
6. Ensure there is an incident reporting policy and required notifications of security incidents are promptly transmitted (Refer to Part E).

[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.

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.

Part A. Authorized Personnel

I. PURPOSE OF THIS SECTION

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.[2]

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.[3]
   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.

[2] 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).

[3] This limits access to CJI to only authorized personnel with the need and the right to know.

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.

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

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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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.

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[8] 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[9] 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.

[8] 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.

[9] 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).

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.[10]

T. The Tribe or TGRA will NOT allow publicly accessible computers[11] to be used to access, process, store, or transmit CJI.

III. SELF-AUDIT

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

[10] 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.

[11] Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

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 C)

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[12] to CJI[13] /CHRI[14] 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.

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

[13] 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.

[14] 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.

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.
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.[15]
   3. Privileged User.[16]
   4. Organizational Personnel with Security Responsibilities.[17]

[15] A user, but not a process, who is authorized to use an information system.

[16] A user that is authorized (and, therefore, trusted) to perform security relevant functions that general users are not authorized to perform.

[17] 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.

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.
   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.[18]

III. SELF-AUDIT

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

[18] CJISSECPOL Awareness and Training (AT)4(b).

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. Implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.
2. Carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.
3. Ensure the information system generates audit records for defined events.[19] These defined events include identifying significant events which must be audited as relevant to the security of the information system application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcome of the events.
4. Periodically review and update the list of agency-defined auditable events.

B. In the event the Tribe or TGRA does not use an automated system, the LASO will manually record activities that are still taking place.

C. 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.

[19] These defined events include identifying significant events which need to be audited as relevant to the security of the information system.

h. Successful and unsuccessful actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.).

i. 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 include the following content with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

E. The LASO will ensure the information system provides alerts to appropriate Tribe or TRGA officials in the event of an audit processing failure.[20]

F. The LASO will designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions at a minimum once a week.[21]

G. The Tribe or TGRA will increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to Tribe or TGRA operations, Tribe or TGRA assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

H. The Tribe or TGRA's information system will provide time stamps for use in audit record generation that include the date and time values generated by the internal system clocks in the audit records.

I. The system clocks will be synchronized on an annual basis.

J. The Tribe or TGRA information system will protect audit information and audit tools from modification, deletion, and unauthorized access.

[20] Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

[21] The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review.

K. The Tribe or TGRA will:

1. Retain audit records for at least one (1) year.
2. Continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.[22]
3. Maintain a log for a minimum of one (1) year on all NCIC and III transactions.

III. SELF-AUDIT

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

[22] This includes, for example, retention and availability of audit records relative to information requests, subpoena, and law enforcement actions.

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. Events and Incident Types[23]

1. Adverse events[24]
2. A security incident is a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. Examples of security incidents are:
   a. An attacker sends high volumes of connection requests to a web server, causing it to crash.
   b. Users open an email that appears to be legitimate but contains malicious software that infects their computers and establishes connections with unknown external host(s).
   c. An attacker obtains sensitive data from a user or organization.
   d. A person gains unauthorized physical access to a secure room containing sensitive documents.

[23] An event is any observable occurrence in a system or network. Events include activities such as a user connecting to a file share, a server receiving a request for a web page, a user sending email, or a firewall blocking a connection attempt.

[24] Events resulting in a negative consequence, such as system crashes, denial of service, unauthorized use of system privileges, unauthorized access to sensitive data, or execution of malware that destroys data.

B. Security Incident Reporting Requirements

1. The Tribe or TGRA will promptly report incident information to appropriate authorities, in accordance with the following:
    a. Security events, including identified weaknesses associated with the event, will be communicated in a manner allowing timely corrective action to be taken.
    b. Wherever feasible, automated mechanisms will be employed to assist in the reporting of security incidents.
    c. When TGRA personnel suspect, or become aware of, any information security incident involving unauthorized access, loss, modification, or disclosure of Tribe or TGRA information or systems for CJIS information, the employee will:
        (1) Immediately notify their supervisor and the LASO. Notification may be done by email and phone, and must include the following:
            i. A Security Incident Report Response Form must be completed and submitted to the employee's supervisor, LASO, and the NIGC Information Systems Officer (ISO) **within 24 hours of discovery of the incident**. The submitted report must contain detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.
            ii. If it is unclear as to whether a situation should be considered a security incident, the Tribe or TGRA LASO should contact the NIGC ISO out of precaution to determine if reporting is required.
            iii. The LASO will review and process all reports of potential security incidents.
        (2) Security incidents involving CJIS systems and/or the actual loss of CJIS provided information will be processed according to the following steps:
            i. The LASO will promptly[25] report the incident information to the TGRA Executive Director.
            ii. The LASO will utilize the Security Incident Response Form when reporting incidents to the FBI CJIS Division.
            iii. Incidents[26] involving outsourced non-channeler contractors must be reported **within one hour of the incident to the NIGC and FBI**.
            iv. **Within five (5) calendar days** of such a report, a written incident report must be provided to the FBI.
            v. Any inadvertent release or compromise of sensitive data that includes CJI, including the loss or compromise of portable computing devices or removable media containing sensitive CJI data, or the discovery of unauthorized access to sensitive CJI data on a computer or storage device, **must be reported immediately** to the LASO and the NIGC ISO.
            vi. For all other non-critical incidents, the LASO will notify the TGRA Executive Director and /or Commission.

[25] Within one hour of becoming aware.

[26] Accidental, policy violations, and intrusions.

2. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of Tribe or TGRA assets and are required to report any security events and weaknesses as quickly as possible to the LASO and or designated point of contact and the NIGC ISO (iso@nigc.gov).

C. Security Incident Response
1. The LASO will ensure identified remediation actions are performed as required, including but not limited to CJISSECPOL. These will include, but are not limited to the following:
   a. Analysis of incident and systems affected.
   b. Identification and analysis of all weaknesses associated with the incident, affected systems, and automated responses (if applicable).
   c. Containment of incident and system weaknesses.
      (1) Address and eradicate intrusion(s) and system weaknesses.
      (2) Upgrade or modify automated responses (if applicable) and/or detection methods (if necessary).
      (3) Recovery actions (if applicable/necessary).

D. Management of Security Incidents
1. A consistent and effective approach will be applied to the management of security incidents. Responsibilities and procedures will be in place to document, investigate, analyze, handle, address, contain, and eradicate security events and weaknesses thoroughly and effectively once they have been reported.

E. Incident Handling
1. The Tribe or TGRA will implement an incident handling capability for security incidents that includes preparation, detection, analysis, containment, eradication, and recovery. Wherever feasible, the Tribe will employ automated mechanisms to support the incident handling process. Incident-related information can be obtained from a variety of sources including, but not limited to audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The Tribe or TGRA will incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly. The Tribe or TGRA will follow NIST SP 800-61r2 standard that is organized into four lifecycle phases in the “Containment, Eradication, Recovery and Post-Incident” procedure.

F. Collection of Evidence

1. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed so that any evidence can be admissible in court. In addition, evidence should always be accounted for. Whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence, including the following:
   a. Identifying information.[27]
   b. Name, title, and phone number of each individual who collected or handled the evidence during the investigation and date/time (including time zone) of each occurrence.[28]
   c. Locations where the evidence was stored.

2. When feasible, establish system snapshots prior to performing investigations and as soon as one suspects that an incident may have occurred. From an evidentiary standpoint, it is much better to get a snapshot of the system as-is rather than doing so after incident handlers, system administrators, and others have inadvertently altered the state of the machine during the investigation. Users and system administrators should be made aware of the steps that they should take to preserve evidence.

G. Incident Monitoring

1. The LASO will track and document security incidents on an ongoing basis. The LASO will maintain completed security incident reporting forms.

H. Incident Response Training

1. The LASO will ensure incident response roles and responsibilities are included and tracked as part of the required entrance on duty and required refresher CJIS awareness and trainings.

I. Distribution and Maintenance

1. This policy will be reviewed at a minimum annually by the LASO. All updates will be distributed and made available to all TGRA staff and employees upon issuance. It will also be distributed to all new TGRA employees and contractors as part of the onboarding process.

III. SELF-AUDIT

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

[27] e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer.

[28] Develop a Chain of Custody Log.

Appendices

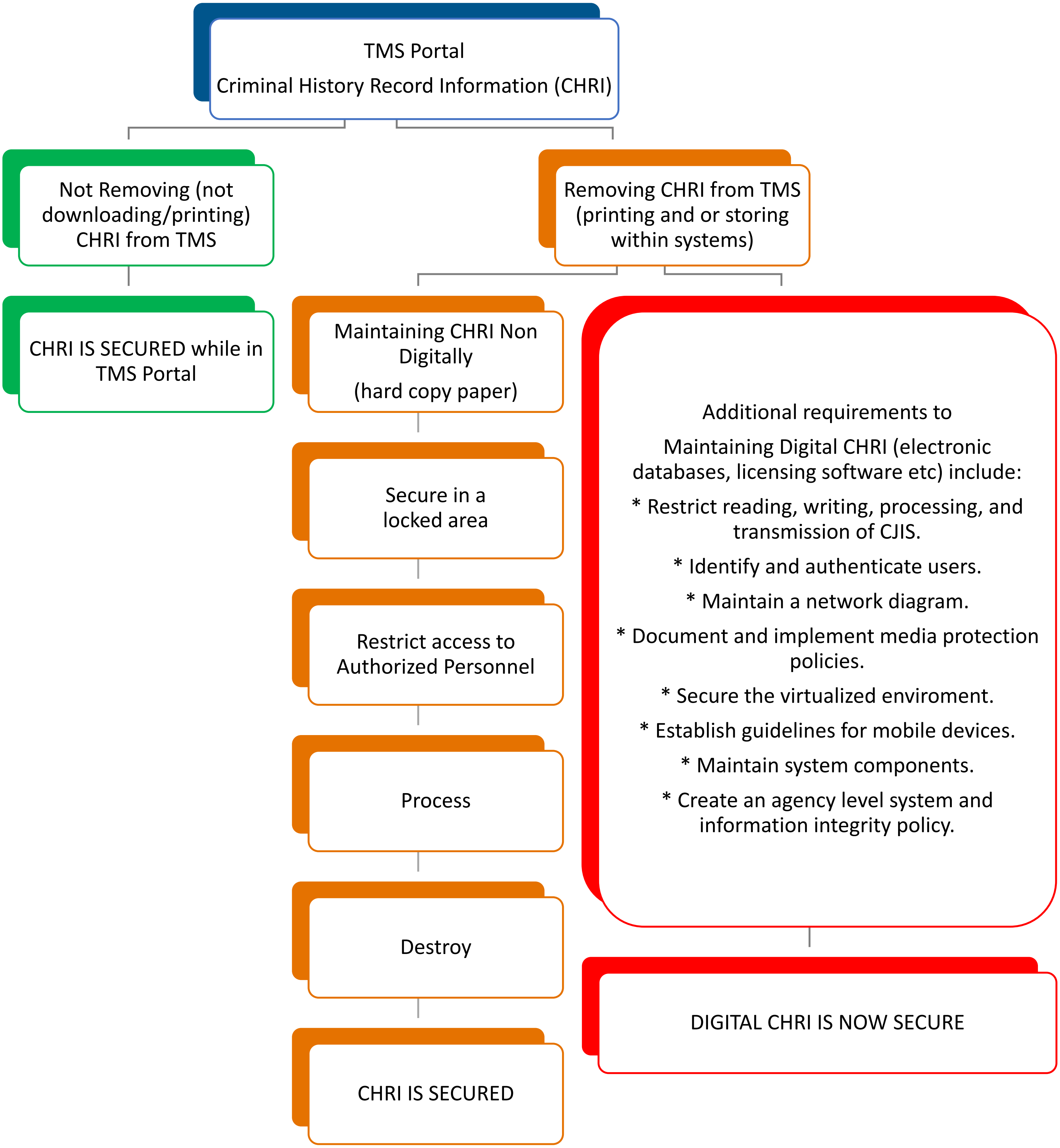
Appendix A- Sample Checklists

CJISSECPOL Sample Checklists:
The CJISSECPOL policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

These sample checklists are audit tools that Tribes can use to self-assess compliance with the CJISSECPOL.

- 2022.5 Sample Audit Checklist CSP 5.1 Version 5.9
- 2023.4 Sample Audit Checklist CJISSECPOL 5.2 Version 5.9.2
- 2022.5 Sample Audit Checklist CSP 5.3 Version 5.9
- 2022.5 Sample Audit Checklist CSP 5.4 Version 5.9
- 2022.5 Sample Audit Checklist CSP 5.5 Version 5.9
- 2022.5 Sample Audit Checklist CSP 5.6 Version 5.9
- 2022.5 Sample Audit Checklist CSP 5.7 Version 5.9
- 2023.4 Sample Audit Checklist CJISSECPOL 5.8 Version 5.9.2
- 2022.5 Sample Audit Checklist CSP 5.9 Version 5.9
- 2022.5 Sample Audit Checklist CSP 5.10 Version 5.9
- 2022.5 Sample Audit Checklist CSP 5.13 Version 5.9
- 2023.4 Sample Audit Checklist CJISSECPOL 5.14 Version 5.9.2
- 2023.4 Sample Audit Checklist CJISSECPOL 5.15 Version 5.9.2

Appendix B- CHRI Storage



TMS Portal

Criminal History Record Information (CHRI)

Not Removing (not downloading/printing) CHRI from TMS

CHRI IS SECURED while in TMS Portal

Removing CHRI from TMS (printing and or storing within systems)

Maintaining CHRI Non Digitally

(hard copy paper)

Secure in a locked area

Restrict access to Authorized Personnel

Process

Destroy

CHRI IS SECURED

Additional requirements to

Maintaining Digital CHRI (electronic databases, licensing software etc) include:

* Restrict reading, writing, processing, and transmission of CJIS.

* Identify and authenticate users.

* Maintain a network diagram.

* Document and implement media protection policies.

* Secure the virtualized enviroment.

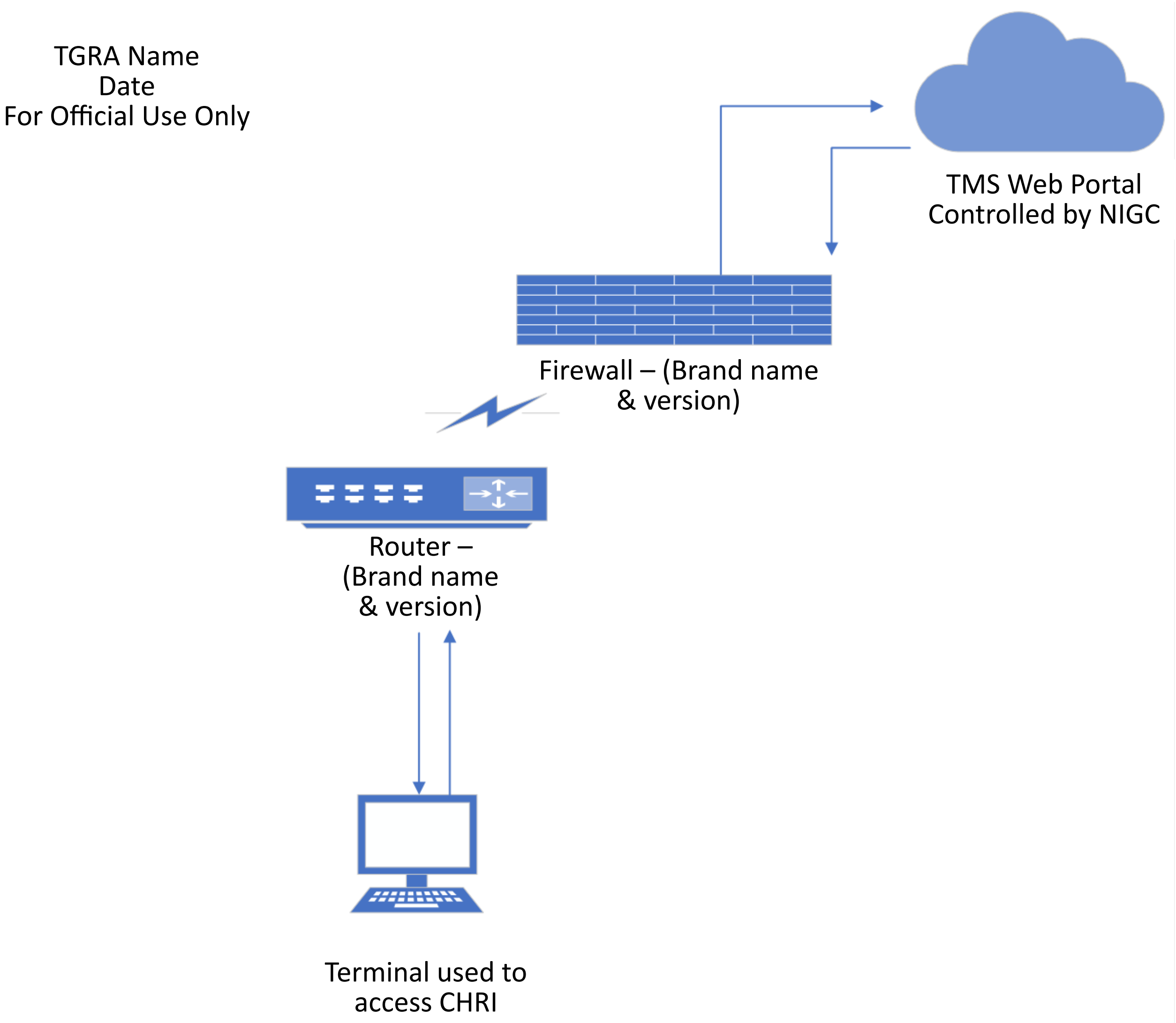
* Establish guidelines for mobile devices.

* Maintain system components.

* Create an agency level system and information integrity policy.

DIGITAL CHRI IS NOW SECURE

Appendix C- Network Diagram SAMPLE


TGRA Name
Date
For Official Use Only
TMS Web Portal
Controlled by NIGC
Firewall – (Brand name
& version)
Router –
(Brand name
& version)
Terminal used to
access CHRI