|  |  |
| --- | --- |
| **INSERT TRIBE / TGRA NAME** | **INSERT TRIBE / TGRA NAME** |
| Criminal Justice Information Services Security Policy Area 5.9 – Physical and Environmental Protection |
| Approval Date: | **Click or tap to enter a date.** | Effective Date: | **Click or tap to enter a date.** |

**I. Purpose**

The purpose of this written process is to document compliance with the Criminal Justice Information Services Security Policy (CJISSECPOL), Policy Area 5.9, Physical and Environmental Protection (PE).

**II. Policy**

The **INSERT TRIBE / TGRA NAME** oversees the implementation of compliance responsibilities identified in the Memorandum of Understanding (MOU) with the National Indian Gaming Commission (NIGC) regarding Criminal History Record Information (CHRI), dated August 2021 (2021 CHRI MOU). The 2021 CHRI MOU was executed by the **INSERT TITLE** and the NIGC on **Click or tap to enter a date.**

This document identifies the **INSERT TRIBE / TGRA NAME** process for PE as identified in CJISSECPOL v5.9.5 dated July 9, 2024, as it relates to authorized personnel access to the NIGC managed [Tribal Management Services (TMS) Portal](https://fp.nigc.gov/) at **INSERT TRIBE / TGRA NAME** Office(s) and or alternate work sites, if explicitly approved by **INSERT TITLE**.

**III. Procedure**

1. **INSERT TITLE** will establish / maintain a current authorized personnel list (APL) with access to CHRI from the NIGC TMS Portal. [2021 CHRI MOU: Guidance Appendix, 4.b]
2. **INSERT TITLE** will submit the APL to the NIGC Information Security Officer (NIGC ISO) (iso@nigc.gov). **INSERT TITLE** will ensure the APL is updated when changes occur and will provide the updated APL to the NIGC ISO when changes occur. [2021 CHRI MOU: Guidance Appendix, 4.b]
3. Authorized personnel access CHRI at the NIGC TMS Portal using a web browser (e.g., Google Chrome, Mozilla Firefox, etc.). Staff view CHRI response(s) from the TMS Portal. Staff do not download or print the CHRI response from the TMS Portal. Consistent with **INSERT TRIBE / TGRA NAME** background and licensing processes, staff verify any applicant CHRI disclosure(s) and/or obtain source record information to verify any reportable criminal charges as identified in 25 C.F.R.§ 556.4 (a)(8), (9) & (10).
4. The **INSERT TRIBE / TGRA NAME** administratively restricts staff web browser access to the NIGC Portal while on duty at the **INSERT TRIBE / TGRA NAME** Office(s) located at **INSERT PREMISE ADDESS(ES)** and other alternative work site(s). Any alternate work site(s) must be approved in advance by the **INSERT TITLE** and comply with all applicable **INSERT TRIBE / TGRA NAME** **INSERT POLICIES AND PROCEDURES**, including this one, and other applicable PE requirements. Written documentation of alternate work site approvals and authorizations will be maintained to demonstrate CJISSECPOL PE compliance. [CJISSECPOL PE-2, PE-3, PE-17]
5. Consistent with the **INSERT TRIBE / TGRA NAME** written process for Media Protection (MP), the **INSERT TRIBE / TGRA NAME** prohibits staff use of personally owned digital media devices to access the TMS Portal. [CJISSECPOL MP-7, b]
6. The **INSERT TITLE** is responsible to maintain and keep current a list of staff and individuals with authorized unescorted and escorted access to the **INSERT TRIBE / TGRA NAME** Office(s) and other alternative work site(s). [2021 CHRI MOU: Guidance Appendix, 10 b, CJISSECPOL PE-2, PE-3, PE-17]
7. Individuals with escorted access are required to sign-in and sign-out at **INSERT LOCATION AND RECORD TYPE**. Individuals with escorted access privileges are required to be physically escorted by authorized staff while in physically secure locations. [2021 CHRI MOU: Guidance Appendix, 10 c, CJISSECPOL PE-3]
8. When at **INSERT TRIBE / TGRA NAME** Office(s), all staff and individuals are required to physically wear / display issued authorization credentials in the physically secure location(s). [CJISSECPOL PE-2, PE-3]
9. **INSERT TRIBE / TGRA NAME** staff and individuals utilize **INSERT CONTROLLING INGRESS AND EGRESS METHODS (E.G., PHYSICAL KEY(S), LOCKS, COMBINATIONS, BIOMETRICS READERS, AND OR CARD READERS, ETC.** to access the physically secure location(s). The physically secure location(s) are designated by the **INSERT TITLE** with prominently posted placards / notices as secured for access and processing of CHRI. [2021 CHRI MOU: Guidance Appendix, 10 a, 10 c, CJISSECPOL PE-3]
10. Issuance of ingress / egress methods and any associated audit logs for the system(s) deployed to control access to the physically secure location(s) are managed and maintained by **INSERT TRIBE / TGRA NAME**. [CJISSECPOL PE-3]
11. The **INSERT TITLE** will review and update this written process annually and following any incident involving unauthorized access to CHRI. [CJISSECPOL PE-1 c]
12. If future business processes include the processing, maintenance, or storage of CHRI on **INSERT TRIBE / TGRA NAME** and/or Contractor[[1]](#footnote-2) outsourced information systems, the **INSERT TITLE** will ensure this written process complies with the PE requirements identified in CJISSECPOL v5.9.5, dated July 9, 2024, and/or the Security and Management Control Outsourcing Standard for Non-Channelers, dated May 16, 2018, as applicable.

**IV. Self-Audit**

1. Complete the [Sample Audit Checklist 5.9 Physical and Environmental Protection](https://www.nigc.gov/images/uploads/2024_04_Sample_Audit_Checklist_CJISSECPOL_5_9_Version_5_9_4.pdf) (PE) as applicable.
2. Complete the [Sample Audit Checklist for Contractor Access to FBI CHRI](https://www.nigc.gov/images/uploads/Sample_90_day_audit_checklist_for_contractor_access_to_FBI_CHRI_from_the_NIGC_Final.pdf) as applicable.

**V. Tracking**

* 1. Identify storage and tracking.
1. Save all compliance documents at **INSERT LOCATION, FILENAME, ETC.**
2. Document compliance status by CJISSECPOL Policy Area at **INSERT LOCATION, FILENAME, ETC.**

D**ocument Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Name** | **Role** | **Change Description** |
| 1.0 | 6/13/2024 | **Steiner, Steven** | **Author** | **Initial written process** |
| 1.1 | 8/15/2024 | **Steiner, Steven** | **Annual update** | **v5.9.5 update, process review** |

1. Contractor means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI. [↑](#footnote-ref-2)