|  |  |  |  |
| --- | --- | --- | --- |
| **INSERT TRIBE / TGRA NAME** | | **INSERT TRIBE / TGRA NAME** | |
| Criminal Justice Information Services Security Policy Area Media 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 Media Protection (MP) requirements.

**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 **INSERT TITLE** and the NIGC on **Click or tap to enter a date.**

The applicable requirements for the maintenance or storage of FBI CHRI from the NIGC are found in the MP requirements identified in [CJISSECPOL Version 6.0 dated December 27, 2024](https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center).

This document affirms the **INSERT TRIBE / TGRA NAME** does not process, maintain, or store FBI CHRI from the NIGC on digital or non-digital media.

**III. Procedure**

1. The **INSERT TRIBE / TGRA NAME** does not allow authorized individuals to use digital or non-digital media to process, maintain or store CHRI. [CJISSECPOL MP-1 a]
2. Authorized personnel access CHRI at the NIGC [Tribal Management Services (TMS) Portal](https://fp.nigc.gov) 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).
3. Authorized personnel ensure browser data history is cleared after each use of the TMS Portal. Clearing TMS Portal history data removes search box history, cookies and other site data, cached images and files from the device utilized to access the TMS Portal.
4. Authorized personnel ensure the **[INSERT DISK CLEANUP ULITIY (E.G., MIRCOSOFT DISK CLEANUP, ETC)]** application is utilized to remove any unintended remaining internet cache files each **INSERT FREQUENCY**.]
5. The **INSERT TRIBE / TGRA NAME** will review and update this written process annually and following any incident if it was determined staff had processed, maintained, or stored CHRI on digital or non-digital media. [CJISSECPOL MP-1 c]
6. Out of an abundance of caution, the **INSERT TRIBE / TGRA NAME** will ensure any digital media utilized to access the TMS Portal is sanitized or destroyed prior to release or disposal. [CJISSECPOL MP-6 a, b]
7. The **INSERT TRIBE / TGRA NAME** administratively prohibits staff use of personally owned digital media devices to access the TMS Portal. [CJISSECPOL MP-7, b]

**IV. Self-Audit**

1. Complete the related NIGC sample audit checklist at [CJIS Resource Materials](https://www.nigc.gov/technology/cjis-resource-materials) as not 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** |
| 1.2 | 03/12/2025 | **Steiner, Steven** | **Update** | **V6.0 update, process review** |