|  |  |  |  |
| --- | --- | --- | --- |
| **INSERT TRIBE / TGRA NAME** | | **INSERT TRIBE / TGRA NAME** | |
| Criminal Justice Information Services Security Policy Area Incident Response | | | |
| 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) Incident Response (IR) 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.**

This document identifies the **INSERT TRIBE / TGRA NAME** process for IR as identified in [CJISSECPOL Version 6 dated December 27, 2024](https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center), as it relates to staff access to the NIGC managed [Tribal Management Services (TMS) Portal](https://fp.nigc.gov/).

**III. Procedure**

1. Consistent with the written process for Access Control (AC), the **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. In accordance with the **INSERT TRIBE / TGRA NAME** AC written process, the **INSERT TITLE** will submit the APL to the NIGC Information Security Officer (NIGC ISO) ([iso@nigc.gov](mailto: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. If **INSERT TITLE** has reason to believe improper access or use of the TMS Portal by staff, the **INSERT TITLE** will contact the NIGC ISO ([iso@nigc.gov](mailto:iso@nigc.gov)) to determine if further analysis of NIGC TMS Portal user account activity logs is necessary. When necessary, the review of NIGC TMS Portal user account activity logs will be conducted by the NIGC ISO and the results of the review will be communicated to the **INSERT TITLE**.
5. If authorized personnel or unauthorized staff misuse or if improper access to FBI CHRI has occurred, the **INSERT TITLE** will investigate, document, and report the incident to the NIGC ISO ([iso@nigc.gov](mailto:iso@nigc.gov)) **within 24 hours of detection**. [2021 CHRI MOU: Guidance Appendix, 7 a, d] [CJISECPOL IR-2 (3), IR-6 b, IR-6 (3), IR-7]
6. Consistent with the written process for Media Protection (MP), the **INSERT TRIBE / TGRA NAME** administratively prohibits staff use of personally owned digital media devices to access the TMS Portal [CJISSECPOL MP-7 b]. If it is determined staff accessed the TMS Portal with a personally owned media device, the INSERT TITLE will investigate, document, and report the incident to the NIGC ISO ([iso@nigc.gov](mailto:iso@nigc.gov)) **within 24 hours of detection**. [2021 CHRI MOU: Guidance Appendix, 7 a, d] [CJISSECPOL IR-2 (3), IR-6 b, IR-6 (3), IR-7]
7. The **INSERT TRIBE / TGRA NAME** utilizes the Security Incident Response Form developed by the FBI CJIS Division and modified by the NIGC titled “F.1 Security Incident Response Form” to report incidents. The current form is available at [NIGC CJIS Resource Materials](https://www.nigc.gov/technology/cjis-resource-materials), Sample Forms and Policies.[2021 CHRI MOU: Guidance Appendix, 7, c] [CJISSECPOL IR-2 (3), IR-6 b]
8. The **INSERT TRIBE / TGRA NAME** will review and update this written process annually and following any incident involving unauthorized access to CHRI. [CJISSECPOL IR-1 c]
9. If improper access or use of the TMS Portal by staff is confirmed by the **INSERT TITLE**, staff will be subject to discipline consistent with the **INSERT APPROPRIATE TRIBE OR TGRA POLICY TITLE**. Repeated TMS Portal user account misuse will result the reassignment of TMS Portal user account roles / privileges to include the removal of access to CHRI from the TMS Portal.
10. The **INSERT TITLE** tracks and documents each incident, including user response activities as identified in this written process at V. Tracking. [2021 CHRI MOU: Guidance Appendix, 7 b] [CJISSECPOL IR-5]
11. 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 IR requirements identified in [CJISSECPOL Version 6.0, dated December 27, 2024](https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center), and/or the [Security and Management Control Outsourcing Standard for Non-Channeling, dated May 8, 2025](https://www.fbi.gov/file-repository/cjis/compact-council-security-and-management-control-outsourcing-standard-for-non-channeling.pdf/view), as applicable. [2021 CHRI MOU: Guidance Appendix, 7 a]

**IV. Self-Audit**

1. Complete the related NIGC sample audit checklist at [CJIS Resource Materials](https://www.nigc.gov/technology/cjis-resource-materials) as applicable.
2. Complete the [Sample Audit Checklist for Outsourcing](https://www.nigc.gov/wp-content/uploads/2025/07/20250723_Sample_Audit_Checklist_for_Outsourcing_Standards_for_Non-Channeling.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** |
| 1.2 | 03/12/2025 | **Steiner, Steven** | **Update** | **V6.0 update, process review** |
| 1.3 | 03/25/2025 | **Steiner, Steven** | **Review** | **Verified updated hyperlink** |
| 1.4 | 07/07/2025 | **Steiner, Steven** | **Update** | **Outsourcing standards updated, verified hyperlinks.** |
| 1.5 | 07/24/2025 | **Steiner, Steven** | **Update** | **New webpage hyperlinks** |

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)