Santa Clara Pueblo Gaming Commission

Noncriminal Justice Agency Policies and Procedures

Revised 6/28/2022

CHAPTER II - LICENSING

SECTION 11: NONCRIMINAL JUSTICE AGENCY POLICES AND PROCEDURES

CHAPTER II – LICENSING

SECTION 11: NONCRIMINAL JUSTICE AGENCY POLICIES AND PROCEDURES

11.1 Purpose. The Commission may use the Criminal Justice Information ("CJI") or Criminal History Record Information ("CHRI") obtained from the NIGC only for the specific purpose of determining eligibility of a person applying for a Key or Primary Management Official gaming license. CJI/CHRI may not be reused for any other purpose.

11.2 Authority. The Commission has the authorization to submit fingerprints to the NIGC for Federal Criminal History Checks pursuant to the Santa Clara Pueblo Gaming Code adopted by the Santa Clara Pueblo Tribal Council Resolution No. 2019-018 and the Memorandum of Understanding between the Commission and the NIGC adopted by Santa Clara Pueblo Tribal Council Resolution 2021-068.

11.3 Local Agency Security Officer (Primary Liaison).

(1) The Commission will designate a Local Agency Security Officer ("LASO") who will be the point of contact with the NIGC through which all communication with the NIGC regarding audits, Tribe/personnel information changes and to ensure training including security awareness training are conducted for authorized personnel. The LASO will maintain all authorized personnel training on the NCJA Training Documentation Form (or similar document). This information will be available at time of audit. The LASO can receive and disseminate communication updates from the NIGC. For the responsibilities of the LASO, refer to the Local Agency Security Officer Basic Responsibilities worksheet in the training handouts.

(2) The LASO will ensure audits are conducted to verify the fingerprint submissions are for the specific purposes of licensing Key or Primary Management Officials. This audit will be performed within thirty (30) days after fingerprint statements have been received from the NIGC. The LASO will determine if an applicant's fingerprint submission was eligible as a Key ("KEY") or Primary Management Official ("PMO") by utilizing the KEY/PMO Classification Checklist worksheet.

11.4 Authorized Personnel.

(1) The Commission staff may encounter CJI/CHRI. Authorized personnel will be given access to view and handle the CJI/CHRI after completing the required training (CJIS Online Security & Awareness training and reading our Tribe- specific policies and procedures) and the one-time signing of an acknowledgment statement. The Authorized Personnel shall consist of the Commission staff, the Santa Clara Pueblo Tribal Administrative IT Department & Custodial personnel and designated Local Agency Security Officer (LASO). Refer to the Authorized Personnel List for the most current authorized personnel. The authorized personnel are aware of the other personnel on this list. Upon termination of authorized personnel, the LASO will update the Authorized Personnel List with the NIGC as soon as possible.

(2) The personnel listed on the current Authorized Personnel List on file with the NIGC Access Integrity Unity (AIU) are the only personnel authorized to access, discuss, use, handle, disseminate, file, log and destroy the CJI/CHRI. To prevent tampering, all terminated personnel, the public, all outside persons and entities are prohibited from handling or having any access to CJI/CHRI for any reason. Secondary dissemination to an outside agency is prohibited.

(3) To prevent unauthorized access or tampering, the fingerprint filing cabinet and drawers are locked throughout the day and one key is secured with the LASO and one other key is secured with the designated authorized personnel. All visitors to the area where CJI/CHRI are kept are accompanied by authorized staff personnel as well.

(4) The Non-Criminal Justice Applicant Fingerprint Card Inventory Sheet(s) must be retained for auditing purposes. The National Indian Gaming Commission is on a three-year auditing cycle and can request to see the previous year's inventory sheets. For example, if the audit is being conducted in 2018, the inventory sheets from 2017 must be made available if requested.

11.5 Fingerprint Card Processing.

(1) The Commission requires that all applicants must provide a valid, unexpired form of government-issued photo identification during the application process and prior to fingerprinting to verify their identity. Accepted forms of primary and secondary identification have been approved through the National Crime Prevention and Privacy Compact Council Identity Verification Program Guide.

(2) Copies of the FBI Notifications will be provided to the applicant prior to fingerprinting.

(3) The Commission requires that all applicants must be fingerprinted if they are applying for a Key or Primary Management Official gaming license. Applicants that have disclosed a conviction will be fingerprinted as well. Applicants are fingerprinted on-site at the Commission office.

(4) If the Commission submits fingerprints electronically, the staff will ensure the correct purpose and authority shall be written on the fingerprints to be submitted.

(5) If the Commission uses fingerprint cards, the staff will take possession of the fingerprint cards and will ensure the correct purpose and authority shall be written on the fingerprint card. The words "Indian Gaming Licensee" shall be written in the reason fingerprinted box. Once the fingerprint card is completed and at no point in time is the fingerprint card to be returned to the applicant.

(6) The fingerprint cards are then placed in a manila folder and then into a locked drawer to be mailed to the NIGC. Only authorized personnel have access to this locked drawer and the key is stored in the LASO's office.

(7) To ensure CHRI MOU Compliance, the Commission agrees to use CHRI solely for the purpose of determining an applicant's eligibility for employment as a Key or Primary Management Official.

11.6 Handling/Retention of CJI/CHRI.

(1) If the Commission submits fingerprints electronically, the fingerprint results from the NIGC are delivered by secure email transmission to the Commission. This email should be considered to contain CJI/CHRI and should only be provided directly to authorized personnel or the LASO. Only authorized personnel will access email that contains the CJI/CHRI.

(2) If the Commissions has mailed fingerprint cards, the fingerprint results from the NIGC are delivered by fax to the Commission. This fax should be considered to contain CJI/CHRI and should only be provided directly to authorized personnel or the LASO. Only authorized personnel will obtain fax that contains the CJI/CHRI.

(3) During the course of eligibility determination, the following steps will be followed:

(a) A summary of the CJI/CHRI are stored electronically or place in the Commission's secure storage device/cabinet.

(b) The CJI/CHRI is accessible only by authorized personnel to review and make an eligibility determination.

(c) After an eligibility determination is complete, the CJI/CHRI is then stored electronically or placed in the Commission's secure storage device/cabinet. These records cannot be released for any public records request.

(d) After the final licensing determination is complete, the CJI/CHRI is archived and stored electronically or placed in the Commission's secure storage device/cabinet which is secure/locked throughout the day and all visitors to the area are accompanied by designated Commission staff or authorized personnel.

(4) The Commission shall retain summaries of CJI/CHRI obtained from electronically submitted fingerprints or mailed fingerprint cards for a period not to exceed three (3) years or CJI/CHRI shall be removed from the Commission's secure storage device/cabinet after a licensing decision or after any appeals process has been completed or CJI/CHRI may be immediately disposed of following preliminary licensing decisions.

11.7 Communication.

(1) Authorized Personnel may discuss the contents of the CJI/CHRI with the applicant in a private secure place and extreme care should be taken to prevent overhearing, eavesdropping or interception of communication. The applicant may not be given a copy of the record or allowed to take a picture of it with an electronic device. The record is for the Commission's use only.

(2) Commission staff will not confirm the existence or non-existence of an individual's criminal history record to the public or to any unauthorized individual. The applicant should be informed that if he/she wishes to challenge the content of the record, they can contact:

(a) For a copy of an FBI criminal history record contact the FBI at 304-625-5590. More information found at https://www.fbi.gov/services/cjis/identity-history-summary-checks.

(3) The Commission provides all applicants the right to review and challenge his/her criminal history record if the applicants deem the information has been inaccurately reported. Each applicant will be provided thirty (30) days and in reasonable circumstances no more than sixty (60) days to provide the Commission authentic documentation that reports the criminal history information accurately and completely. This information must be provided prior to eligibility determination of KEY or Primary Management Official gaming license.

(4) CJI/CHRI shall not be copied, emailed, faxed or scanned nor disseminated to secondary parties or the Commission staff. Any casual unauthorized release of information is not allowed (i.e. social media, discussion with friends or family members). CJI/CHRI shall only be discussed (written or verbally) between the authorized personnel as necessary to carry out the specific purpose for which the information was requested and all verbal discussions take place in private.

(5) If the fingerprint-based check has a disqualifying factor, the authorized personnel who opened and reviewed the record will discuss the contents of the record with the applicant in a private and secure manner to obtain any additional information.

11.8 Storage of CJI/CHRI.

(1) Once the CJI/CHRI has met its purpose, it may be stored electronically or placed in the Commission's secure storage device/cabinet by authorized personnel. CJI/CHRI are retained in accordance with the Commissions record retention policy as mentioned above in Section 12.6 Handling/Retention. This CJI/CHRI secure storage device/cabinet does not contain any other employment records or any files which may be considered public record to prevent unauthorized access or dissemination. The secure storage device/cabinet is locked throughout the day to prevent unauthorized access by non-authorized personnel. Access to the secure storage device/cabinet are kept secure by the LASO and/ or other authorized personnel. Only authorized personnel are allowed access to the secure storage device/cabinet that contain the CJI/CHRI. If access to the secure storage device/cabinet that contains the records is lost, the secure storage device/cabinet will be reprogrammed/re-keyed to prevent unauthorized access.

(2) Authorized personnel are responsible for safeguarding the confidentiality of the information at all times and may not disclose or allow access to the information to anyone except authorized personnel. CJI/CHRI is always secured and never left unattended.

(3) If the actual copy of the CJI/CHRI results are not electronically stored, but as mentioned above in Section 12.6 Handling/Retention of CJI/CHRI, some essential information is entered for reference and tracking purposes and electronically stored. Physical protection of CJI/CHRI as well as a physically secure location for CJI/CHRI will be shared and verified with the NIGC. The database where the CJI/CHRI is stored is in the Commission's server which is secure, encrypted and controlled directly by the Commission.

No other organization has access to this database. All visitors to the area where CJI/CHRI are stored electronically are accompanied by authorized personnel.

11.9 FBI Notifications.

(1) The Commission staff will provide copies of the Noncriminal Justice Applicant's Privacy Rights and FBI's Privacy Act Statement to the applicant when they arrive to be fingerprinted and will also be included with the gaming license application. Copies of these FBI Notifications are available at the Commission office, and it will contain the following information:

(a) Your fingerprints will be used to check the criminal history records of the FBI. If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before officials deny you the employment, license, or other benefits based on information in the FBI criminal history record.

(b) The procedures for obtaining a change, correction or updating of your FBI criminal history record are set forth in Title 28 Code of Federal Regulations, section 16.30 through 16.34. Information on how to review and challenge your FBI criminal record can be found at https://www.fbi.gov/services/cjis/identity-history-summary-checks.

11.10 Disposal of CJI/CHRI.

(1) When the CJI/CHRI has met the destruction date in accordance with the Commission's record retention policy as mentioned above in Section 12.6 Handling/Retention, authorized personnel will destroy the CJI/CHRI.

(a) Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

(i) CJI/CHRI will be shredded using Commission shredders.

(ii) CJI/CHRI will be placed in locked shedding receptacle for third-party contractor to come on-site and shred.

(iii) CJI/CHRI will be incinerated using Commission incinerators or witnessed by the Commission authorized personnel on site or at a contractor incineration site.

(b) Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the following methods:

(i) Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

(ii) Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common

magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

(iii) Destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

(2) IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from the Commission's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

(3) In the event of a third-party contractor that performs any destruction process, authorized personnel will accompany the vendor to oversee the handling and disposal of the CJI/CHRI. The authorized personnel, will observe the contractor from the time the receptacle is delivered through the complete destruction of the CJI/CHRI.

11.11 Misuse of CJI/CHRI.

(1) In the event of deliberate, reckless or unintentional misuse of CJI/CHRI, or if the fingerprint submission of any applicant is deemed ineligible, the authorized personnel will be disciplined in accordance with the signed acknowledgment statement and the Commission's disciplinary policy which can include termination.

(2) In the event of any breach of information related to CJI/CHRI, the LASO will report to the NIGC a notification of findings in accordance with the Commission's security incident policy.

11.12 Training and Acknowledgment Statements.

(1) All authorized personnel must be trained in the online security awareness (CJIS Online) training within six months of hire (or upon being added to the Authorized Personnel List) and then every two years thereafter. The LASO must complete training required prior to assuming the LASO duties and every year thereafter.

(2) All authorized personnel must be trained in all in-house privacy and security training on the access, use, handling, dissemination and destruction procedures regarding CJI/CHRI within six months of hire (or upon being added to the Authorized Personnel List) and then every two years thereafter.

(3) All authorized personnel will sign an acknowledgment statement regarding the notification of the penalties for misuse of CJI/CHRI.

(4) All training and acknowledgment statements will be recorded on a training documentation form. This form is reviewed during audits by the NIGC.

(5) All documentation of training and acknowledgment statements of all authorized personnel will be retained for two years. This information is reviewed during audits by the NIGC.

11.13 Outsourcing Agreements.

(1) The Commission will submit a request letter to the FBI Compact Council for consideration of approval of an outsourcing agreement with any third-party (i.e., entity, contractor, or vendor) with access to CJI/CHRI.

(a) To contract noncriminal justice administrative functions to a third-party, including the casino's or tribe's Information Technology (IT) department needed to maintain the network, servers or computers which access and store CHRI, an outsourcing agreement must be drafted and submitted to the FBI Compact Officer, copying the NIGC ISO at iso@nigc.gov, for approval prior to executing the agreement and engaging the service.

(b) The contract must contain the specific noncriminal justice administrative functions to be performed by the third-party that involve access to CJI/CHRI on behalf of the Commission.

(2) Upon receiving approval from the FBI Compact Officer, the Commission and third-party can execute the approved draft contract.

(3) The Commission will perform an audit of the contract and the third-party's compliance with Criminal Justice Information Services Security Policy within 90 days of execution of the contract (when the third-party first receives CJI/CHRI) and certify compliance to the FBI Compact Officer.

(4) Examples of when Outsourcing Agreements are needed:

(a) Shredding: If a TGRA wants to employ a shredding company to destroy CHRI and/or summary CHRI at the TGRA location or are allowed to leave with the documents, an approved outsourcing contract is required.

(b) Storage: If the Tribe uses an off-site storage facility for document storage including CHRI or summary CHRI and storage facility employees have access to CHRI in the box or the facility employees store the CHRI in a locked container that they control, an outsourcing contract is required.

(c) Public Telecom Carriers: If the Tribe uses a public telecom service, which has access to servers, or provide patches to the servers where CHRI is stored, an outsourcing contract is required. If the telecom service does not have access to the servers or provide patches, outsourcing is not required, which is typically the case.

(d) Electronic Media: If a third party stores electronic CHRI data for a Tribe an outsourcing contract is required.

(e) Live Scan Vendors: If a NIGC-approved live scan vendor solely provides live scan service to the Commission and does not have access to CHRI, an outsourcing contract is not needed. However, if the live scan vendor has access to CHRI (this includes any indication that a FBI CHRI record exists or does not exist for a given applicant) or provides services over and above live scan activities, including but not limited to - data storage of CHRI,

network maintenance, or licensing applications where CHRI is stored or summary CHRI information is documented - an outsourcing agreement is required.

If the tribe receives and/or stores CHRI results on the same laptop or computer the live scan device is uses to send the fingerprints to NIGC and the live scan vender has, at any point in time, access, escorted or unescorted, to the CHRI information, an outsourcing agreement is required.

If the tribe purchased the laptop from the live scan vender and has a service agreement for the laptop where CHRI results are received and/or stored, an outsourcing agreement is required.

In summary, if any entity, contractor, or vendor has access to electronic summary CHRI data in electronic or hard-copy form, an outsourcing contract is required.