TTBIA Operations Manual

Title	**Criminal Justice Information (CJI) Systems and Data**
TTBIA Deputy Director Approval Date	**Jeff Hatch 04/10/18**

1.000 Purpose

This policy is intended to provide guidance and direction for Tulalip Tribes Background Investigation Agency (TTBIA) personnel to ensure proper security, access and usage of Criminal Justice Information (CJI) systems and data.

1.010 Scope

These procedures apply to all TTBIA personnel when accessing CJI systems and data as part of performing Tulalip Government employee background investigations, specifically pertaining to Public Law 101-630.

1.020 CJI Security Requirements

1. TTBIA will prominently post signage designating the licensing office as a physically secure area.
2. All visitors to the inside of the TTBIA office housing any CJI system must be accompanied by TTBIA authorized personnel, or TTBIA personnel must be present in the office.
3. Any time TTBIA personnel leave the office empty, they will ensure that the door is closed and locked.
4. Any computer monitors attached to a CJI system must be faced away from windows, doors or hallways, and positioned in such a way that prevents unauthorized viewing.
5. TTBIA will maintain a listing of individuals authorized to access areas containing sensitive devices, data or systems. Any changes to the listing will be updated and notice provided as applicable.
6. TTBIA shall implement password rules for any CJI system to include the following security measures:
   - A. Passwords must be strong and shall be individual to personnel and not be shared with others. Passwords cannot be left in conspicuous locations (keyboard, monitor, mousepad, etc.).
   - B. Password protected screen-saver programs should be activated or the computer locked when stepping away from the system.
   - C. Log off the software/system at the end of a shift or when another operator needs to access the software/system.
7. TTBIA will maintain an up-to-date network diagram for review and audit purposes.
8. If required, TTBIA will take necessary steps to ensure the CJI system is protected by ensuring antivirus software and computer patching are up to date.

TTBIA Operations Manual

Title	Criminal Justice Information (CJI) Systems and Data
TTBIA Deputy Director Approval Date	Jeff Hatch 04/10/18

1.030 CJI Sensitive Information

1. CJI is considered sensitive information and should be safeguarded to prevent unauthorized or improper access, use or dissemination and release of information.
2. Access to CJI is limited to assigned tasks and duties. TTBIA personnel will be held accountable for any and all actions whiles accessing or using CJI.
3. Any unauthorized requests, receipt, release, interception, dissemination or discussion of CJI may result in criminal prosecution and/or termination of employment. Continued misuse of CJI could subject the TTBIA to the cancellation of access to CJI.
4. CJI (CHRI) received as a result of employment purposes, pursuant to Public Law 101-630 can only be used for the purpose for which the record was requested.
5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. TTBIA personnel will be prohibited from printing hard copies of CJI, unless an individual is challenging the accuracy of their criminal history information.
7. FBI Fingerprint results are accessed using LEEP accounts only and the results are not to be printed or stored locally.
8. Application access will utilize unique usernames and passwords, with passwords expiring every 90 days.
9. Authorized vendors will use secure, encrypted VPN software to access applications to provide support only.
10. Only authorized personnel have access to servers and storage media containing confidential data.
11. Authorized personnel (including vendors) must take the CJIS Security Awareness Training.
12. Servers and storage media are located in a secure room under camera coverage with access restricted to only authorized personnel.
13. All CJI data is only stored on the TAP workstation.
14. Server event logs are maintained for 12 months and reviewed weekly.
15. Hard drives are re-formatted three times by authorized personnel prior to disposal and are destroyed by shredding, witnessed by authorized personnel.

1.040 Dissemination of Information

1. It is prohibited to knowingly disseminate CHRI outside of the TTBIA.
2. CHRI electronically returned to TTBIA will not be disseminated to the originating or serviced Tribal Government department. It will only be described in written correspondence from the TTBIA to the

Government Employment department whether the person is eligible or ineligible; based on criteria of the Tulalip Tribes Background Investigations Policy and Tier I-C-Child.

1.050 Administrative Responsibilities

1. An applicant or employee shall be afforded the opportunity to complete, or challenge the accuracy of, the information contained in the FBI Identification record. Suitability determinations should not deny employment based on information in the record until the applicant or employee has been given a reasonable time to correct or complete the record, if inclined to do so.
2. Any employee found to be ineligible for a position, current or pending, may appeal such decision in accordance to the BI Policy and applicable HR administrative process.

1.060 Security Incident Response

1. A SIRC will meet in the event of a data or security breach. This committee will consist of Management, IS Staff and TDS IS Staff who are CJIS Security certified. In the event of a breach, the individuals listed below shall meet at a designated location; room A253 unless instructed otherwise. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. They will determine the severity of the situation and will cooperatively decide which set of procedures to follow based on the type of incident and information available at that time.

   The SIRC consists of the following personnel:
   a) Jeff Hatch (TTBIA Deputy Director/Information Security Officer (ISO))
   b) Sharon Forbes
   c) Lance Ledford
   d) Chris Songer & Michelle Fleek (IS Inspectors)
   e) Jason Read (TDS Network Administrator)

2. These standard operating procedures will be utilized by the Tulalip Tribal Background Investigations Agency in the event of a data or security breach situation. Paramount is the retention and safe-keeping of confidential information.

3. This applies to all TTBIA personnel in cooperation with the SIRC.

4. This policy mandates that any individual who suspects that a theft, breach or exposure of protected or sensitive data has occurred, must immediately provide a description of what occurred by calling 360-716-2040 or 360-716-2013.

5. The TTBIA Deputy Director shall notify Tulalip Data Services (TDS) on all emergency events.

6. Definitions:

   A data breach is defined as an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service with intent to steal and/or publish data to an unsecured or illegal location.

   A security breach is defined as an incursion into a computer or network of computers, usually by hackers or malicious software that compromises sensitive data or causes damage to servers, computers or network function.

7. There are multiple types of security threats:
   a. Malware: Malware is short for “malicious software.” Malware is a term used to mean a “variety of forms of hostile, intrusive, or annoying software or program code.” Malware could be computer viruses, worms, Trojan horses, dishonest spyware, and malicious rootkits.
   b. Computer virus: A computer virus is a small piece of software that can spread from one infected computer to another. The virus could corrupt, steal, or delete data on your computer—even erasing everything on your hard drive. A virus could also use other programs like your email program to spread itself to other computers.
   c. Rogue security software: This is usually a pop-up window that advertises a security update or alert. It appears legitimate and asks you to click on a link to install the “update” or “remove” unwanted malicious software that it has apparently detected. This could be rogue security software designed to lure people into clicking and downloading malicious software.
   d. Trojan horse: Users can infect their computers with Trojan horse software simply by downloading an application they thought was legitimate but was in fact malicious. A Trojan horse can do anything from record your passwords by logging keystrokes (known as a keystroke logger) to hijacking your webcam to watch and record your every move.
   e. Malicious spyware: Malicious spyware is used to describe the Trojan application that was created by cybercriminals to spy on their victims. An example would be keylogger software that records a victim’s every keystroke on the keyboard. The recorded information is periodically sent back to the originating cybercriminal over the Internet.
   f. Computer worm: A computer worm is a software program that can copy itself from one computer to another, without human interaction. Worms can replicate in great volume and with great speed.
   g. Botnet: A botnet is a group of computers connected to the Internet that have been compromised by a hacker using a computer virus or Trojan horse. An individual computer in the group is known as a “zombie“ computer. The botnet is under the command of a “bot herder” or a “bot master,” usually to perform nefarious activities. This could include distributing spam to the email contact addresses on each zombie computer, for example. If the botnet is sufficiently big in number, it could be used to access a targeted website

simultaneously in what's known as a denial-of-service (DoS) attack. The goal of a DoS attack is to bring down a web server by overloading it with access requests.

h. Spam: Spam in the security context is primarily used to describe email spam —unwanted messages in your email inbox. Spam messages can contain links that when clicked on could go to a website that installs malicious software onto your computer.

i. Phishing: Phishing scams are fraudulent attempts by cybercriminals to obtain private information. Phishing scams often appear in the guise of email messages designed to appear as though they are from legitimate sources. For example, the message would try to lure you into giving your personal information by pretending that your bank or email service provider is updating its website and that you must click on the link in the email to verify your account information and password details.

j. Rootkit: A rootkit is a collection of tools that are used to obtain administrator-level access to a computer or a network of computers. A rootkit could be installed on your computer by a cybercriminal exploiting a vulnerability or security hole in a legitimate application on your PC and may contain spyware that monitors and records keystrokes.

8. The following procedure is intended to provide guidance and direction in determining how TTBIA will respond when a data breach or security breach is discovered.

Step	Performed By	Task Description
1.	IS Inspector	A. Notify the TTBIA Deputy Director & SIRC team B. Determine whether a true breach has occurred and its potential impact. A. Identify the nature, scope, impact and origin or root cause of the breach. B. Remove all access to the workstation or server to prevent confidential information from being exported from workstations or servers. C. Collect evidence regarding the breach.
2.	TDS IS Staff	A. Assist in detecting how security was breached. B. Assist in collecting evidence regarding the breach. C. Assist in responding to ongoing threats. D. Recommend security procedures and enhancements.
3.	TTBIA Management	A. Provide clear and immediately communication about what happened and steps staff should take. B. If necessary, develop messaging and deployment schedule for notifying those whose data was compromised based on legal counsel.

4.	IS Inspector	A. Write report. This report will include; a. Date of incident b. Location of incident c. Systems affected d. Method of detection e. Nature of incident f. Description of incident g. Actions taken/resolution B. Educate staff on data breach and security threat prevention.

9. The ISO for TTBIA will notify and provide a completed incident report to the applicable CJIS representative.