# FARIBAULT POLICE DEPARTMENT

| | |
|---|---|
| Policy #609 | Subject: Operational Polices and Standard Operation Procedures |
| Issued by: Chief Andy Bohlen | |
| Personnel: All Personnel | Date Issued: May 21, 2020 |

## Policy: 1.3 – Relationship to Local Security Policy and Other Policies

The agency has reviewed the new FBI CJIS Security Policy V5.8 (June 1, 2019) (www.fbi.gov/services/cjis/cjis-security-policy-resource-center) and is aligning operational policies and standard operation procedures. As part, the agency will maintain written procedures of actions implemented for review upon request

## Policy: 4.3 – Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record 8/4/2014 CJISD-ITS-DOC-08140-5.3 13 for example inherently contains PII as would a Law Enforcement National Data Exchange (NDEx) case file. PII shall be extracted from CJI for the purpose of official business only.

As needed, the agency will continue to develop policies, based on changing state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.

## Policy:  5.1.1 – Information Exchange

The agency use of CJI is only for the purpose of the agency and its employee's abilities to perform their job duties.

Any Disseminating or sharing CJI with anyone that is not authorized to have access to the information is strictly prohibited.

If the agency is releasing the CJI to another authorized agency, a dissemination log will be kept.

## Policy:  5.1.1.1 – Informational Handling

Covered in 5.8 Policy Area 8: Media Protection (page 11).

## Policy:  5.3 – Policy Area Incident Response

The agency will promptly report incident information to the appropriate party.

The agency will disconnect the infected workstation.

The agency will maintain all records around information security events.

Other information collected for completing the Incident Response Form is below:

- Suspected cause for incident (Name of the malware, virus, etc.)
- Was Antivirus software running at the time of infection?
- How and when the problem was first identified?
- When was IT staff been notified?
- Number of workstations infected?
- Any other equipment infected?
- Action plan for removal.
- Was any CJIS data or personnel identification information compromised?
- Once free from infection the system can be reconnected.

**Please see the incident response reporting form on the next page**

# INCIDENT RESPONSE FORM
# REPORTING FORM

DATE OF REPORT:_____ DATE OF INCIDENT: _____

REPORTING PERSON:_____

PHONE:_____ E-MAIL:_____

LOCATION(S) OF INCIDENT:_____

_____

SYSTEM(S) AFFECTED:_____

METHOD OF DETECTION:_____

NATURE OF INCIDENT:_____

INCIDENT DESCRIPTION:_____

ACTIONS TAKEN/RESOLUTION:_____

PERSONS NOTIFIED:_____

_____

## Policy: 5.5.6 – Remote Access

The agency does not authorize remote access to the information system

The agency may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access.

Any exception shall be written and authorized by the head of the agency.

## Policy: 5.5.6.1 – Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g. and agency's public website that contains purely public information).

1. A personally owned information system shall not be authorized to access, process, store or transmit CJI.

2. Personally owned network equipment shall not be authorized to access, process, store or transmit CJI or be attached to any CJE.

3. Any exception shall be written and authorized by the head of the agency.

4. Failure to comply with these policies may result in the loss of access, criminal prosecution and/or administrative action including termination of employment.

## Policy: 5.6.2 – Authentication Policy and Procedures

The agency shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

- Be a minimum length of eight (8) characters on all systems.
- Not be a dictionary word or proper name.
- Not be the same as the User ID.
- Expire within a maximum of ninety (90) calendar days.
- Not be identical to the previous ten (10) passwords.
- Not be transmitted in the clear outside the secure location.
- Not be displayed when entered.

## Policy:  5.6.3.2 – Authenticator Management

The agency shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

- Be a minimum length of eight (8) characters on all systems.
- Not be a dictionary word or proper name.
- Not be the same as the User ID.
- Expire within a maximum of ninety (90) calendar days.
- Not be identical to the previous ten (10) passwords.
- Not be transmitted in the clear outside the secure location.
- Not be displayed when entered.

## Policy:  5.8 – Policy Area 8: Media Protection

The agency will do the following:

- Securely store electronic and physical media within a physically secure or controlled area
- Restrict access to electronic and physical media to authorized individuals.
- Ensure that only authorized users remove printed form or digital media.
- Physically protect media end of life
- Insure end of life media is destroyed or sanitized.
- Not use personally owned information system to access, process, store, or transmit CJI unless the it has established and documented the specific terms and conditions for personally owned information system usage.
- Not utilize publicly accessible computers to access, process, store, or transmit media.
- Store all hardcopy CJI printouts maintained in a secure area accessible to only those employees whose job function require them to handle such documents.
- Safeguard all media against possible misuse by complying with all other policies.
- Take appropriate action when in possession of CJI while not in a secure area:

The agency will insure that media at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption certified to meet FIPS 140-2 standards.

The agency will require users to lock or log off computer when not in immediate vicinity of work area to protect access.

## Policy:  5.8.3 – Digital Media Sanitization and Disposal

The agency will insure that the sanitization of electronics media or the destruction of inoperable media (via incineration, shredding, disintegrating, cutting, drilling, or grinding) is witnessed or carried out only by authorized personnel.

The agency will require for the sanitization of media that the data clearing be done with an approved disk wiping utility using a minimum of three passes or a Security Service (NSA/CSS)-approved degausser.

The agency shall maintain written documentation and logs of the steps taken to sanitize or destroy electronic media.

## Policy:  5.8.4 – Disposal of Physical Media

The agency will insure that the disposal of physical media is done through Physical destruction (via incineration, shredding, disintegrating, cutting, drilling, or grinding).

The agency will insure this is witnessed or carried out only by authorized personnel.

## Policy:  5.9 – Policy Area 9: Physical Protection

The agency will limit who has access to the physically secure location to only those personnel authorized by the agency.

The agency will lock all areas, rooms, or storage containers when unattended.

The agency will position information system devices and documents in such a way as to prevent unauthorized individuals from access and view.

The agency will follow the encryption requirements found in section for electronic storage (i.e. data “at rest”).

## Policy:  5.10.1.2.3 – Public Key Infrastructure (PKI) Technology

The agency shall require for the issuance of public key certificates used in the information system that in order to receive a public key certificate it was authorized by a supervisor or a responsible official and that it is accomplished by a secure process that verifies the identity of the certificate holder.

## Policy:  5.10.4.1 – Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall ensures prompt installation of newly released security relevant patches, service packs and hot fixes.

When able testing of appropriate patches will occur before installation.

**Note:** Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

## Policy:  5.10.4.4 – Security Alerts and Advisories

The agency reviews information system security alerts/advisories on a regular basis.

The agency issues alerts/advisories to appropriate personnel.

The agency documents the types of actions to be taken in response to security alerts/advisories.

The agency used automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

## Policy:  5.12.4 – Personnel Sanctions

If the agency becomes aware of an employee using a CJDN terminal, CJDN terminal generated information, CJDN equipment, or CJDN access in a manner that is not in accordance with the employee's job and the problem is deemed merely operator error or substandard job performance, the agency will contact the employee and advise him/her of the problem and provide additional training to correct the issue.

If the above step does not rectify the problem, or the problem is deemed to be greater than mere operator error or sub-standard job performance, the agency will report the misuse immediately to a supervisor.  The agency will suspend the employee's CJDN access until the supervisor conducts an investigation.

If the investigation does not substantiate that the employee was in violation, the agency will reinstate the employee's CJDN terminal access.

If the investigation substantiates that the employee was in violation, then Disciplinary action may be taken against the employee in accordance with applicable labor agreements.

If the misconduct is deemed to be criminal, the agency will report the behavior of criminal nature to the appropriate party to determine the appropriate action.