REVISED GUIDELINE - VOL. 31, NO. 2

CRIMINAL JUSTICE INFORMATION SECURITY (NON-CRIMINAL JUSTICE AGENCY

In conjunction with Policy 8321, the following procedures and protocols shall be used to provide for the security, confidentiality, and integrity of criminal history records ("CHRI") received from the Michigan State Police and criminal justice information ("CJI") received from the Federal Bureau of Investigation.

Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of District's entire network. As such, all District employees (including contractors and vendors with access to District systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

Scope

This protocol includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any District facility which has access to or stores any non-public criminal history or criminal justice information.

General

A. All system-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every ninety (90) days.

B. If applicable, all production system-level passwords must be part of the Information Security administrated global password management database.

C. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every ninety (90) days.

D. User accounts with access to National Crime Information Center (NCIC) privileges must have a unique password from all other accounts held by that user.

E. Passwords must not be inserted into email messages or other forms of digital communication.

F. Where simple network management protocol (SMTP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system" and must be different from passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

G. All user-level, system-level, and NCIC access level passwords must conform to the guidelines described below.

Password Guidelines

A. Avoid poor, weak passwords which have the following characteristics:

1. The password contains less than eight (8) characters.

2. The password is a word found in a dictionary (English or foreign).

3. The password is a common usage word such as:

a. names of family, pets, friends, co-workers, fantasy characters, etc.

b. computer terms and names, commands, sites, companies, hardware, software

c. the words "District," "WVSP," "HPD," "CKSFP" or any derivation

d. birthdays and other personal information such as addresses and phone numbers

e. word or number patterns like aaabbb, 111222, zyxwvts, 4654321, etc.

f. any of the above spelled backward like nhoj, yrrehckcalb, yffulf, etc.

g. any of the above preceded or followed by a digit (e.g., secretl, lsecret)

B. Use strong passwords which have the following characteristics:

1. contain both upper and lower case characters (e.g., a-z, A-Z)

2. have digits and punctuation characters as well as letters, e.g., 0-9. !@#$%^&()_+{}[]:";<>?,.?

3. are at least eight (8) alphanumeric characters long

4. are not a word within any language, slang, dialect, jargon, etc.

5. are not based on personal information, names of family, etc.

6. passwords based on a song title, affirmation, or other phrase For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "TmblW>r~"or some other variation. **NOTE: Do not use either of these examples as passwords**

Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

A. when a user retires, quits, is reassigned, released, dismissed, etc.

B. default passwords shall be changed immediately on all equipment

C. contractor accounts, when no longer needed to perform their duties

When a password is no longer needed, the following procedures should be followed:

A. Employee should notify his/her immediate supervisor.

B. Contractor should inform his/her point-of-contact (POC).

C. Supervisor or POC should fill out a password deletion form and send it to the District's Local Agency Security Officer (LASO).

D. LASO will then delete the user's password and delete or suspend the user's account.

E. A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended.

F. The password deletion form will be filed in a secure filing system.

Password Protection Standards

Do not use your User ID as your password. Do not use the same password for District accounts as for NCIC accounts. For example, select one password for your Windows account login and a different one for your NCIC account login. Do not share District passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential District information.

Here is a list of "do not's":

A. Don't reveal a password over the phone to anyone.

B. Don't reveal a password in an e-mail message.

C. Don't reveal a password to the boss.

D. Don't talk about a password in front of others.

E. Don't hint at the format of a password (e.g., "my family name").

F. Don't reveal a password on questionnaires or security forms.

G. Don't share a password with family members.

H. Don't reveal a password to a co-worker while on vacation.

I. Don't use the "Remember Password" feature of applications.

J. Don't write passwords down and store them anywhere in your office.

K. Don't store passwords in a file on ANY computer system without encryption.

If someone demands a password, refer them to this document or have them call the LASO.

If an account or password is suspected to have been compromised, report the incident to the LASO and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the FBI or MSP. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Application Development Standards

Application developers must include the following security precautions in their programs:

A. authentication of individual users, not groups

B. no storage of passwords in clear text or in any easily reversible form

C. support for Terminal Access Controller Access Control System+ (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible

Session Lock

The information system (computer, etc.) shall prevent further access to the system by initiating a session lock after a maximum of thirty (30) minutes of inactivity, and the session lock shall remain in effect until the authorized user re-establishes access using appropriate identification and authentication procedures. Authorized users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. Note: an example of a session lock is a screen saver with password.

Remote Access Users

Access to the District networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and User ID are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.). Access to the District networks via personal communication devices ("PCDs") shall be strictly controlled and authorized.

Encryption

When encryption is required under Policy 8321, it shall comply with the following standards and procedures.

A. Encryption shall be a minimum of 128 bit.

B. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

EXCEPTIONS:

1. Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public.

2. CJI transmitted via facsimile is exempt from encryption requirements.

C. When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).

D. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

1. Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

2. Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

3. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

    a. Include authorization by a supervisor or a responsible official.

    b. Be accomplished by a secure process that verifies the identity of the certificate holder.

    c. Ensure the certificate is issued to the intended party.

Disposal of Media Procedures

When no longer usable, diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items used to process or store classified and/or sensitive data, including CHRI, shall be properly disposed of in accordance with measures established by the District. The following procedures will be followed:

A. When no longer usable, hard copies and print-outs shall be placed in properly marked shredding bins located in a secure location only accessible by authorized individuals.

B. Diskettes and tape cartridges shall be taken apart and placed in the properly marked shredding bins.

C. After media has been shredded it will be placed in appropriate bins to be incinerated or disposed of properly.

IT systems that have processed, stored, or transmitted sensitive and/or classified information shall not be released from <Agency Name's> control until the equipment is sanitized and all stored information has been cleared. For sensitive, but unclassified information, the sanitization method shall be approved by the District. For classified systems, National Security Association approved measures shall be used. The following procedure will be followed:

A. Employees will send all hardware that processes and/or stores classified and/or sensitive data to the District <Security Personnel> to be properly disposed.

B. The District's Technology Director will dispose of hardware by one of the following methods:

1. **Overwriting** - 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. The number of times the media is overwritten depends on the level of sensitive information but must be a minimum of three (3) times if CHRI.

2. **Degaussing** - a method to magnetically erase data from magnetic media. Two (2) 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.

3. **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.

Also, computers that are used to transmit classified and/or sensitive information must protect residual data. This can be accomplished with the use of integrated encryption technology. This technology uses a device or software which encrypts all data as it is written to the disk. When the user retrieves a file, the data is automatically decrypted for the owner to use. This encryption/decryption process is

typically transparent to the user. Should the hard drive be removed, no usable data can be retrieved.

Mobile Devices

At a minimum, the District shall ensure that all mobile devices used for accessing CJI:

A. apply available critical patches and upgrades to the operating system as soon as they become available for the device;

B. are configured for local device authentication;

C. use advanced authentication;

D. encrypt all criminal justice information on the device;

E. erase all cached information when session is terminated;

F. employ personal firewalls or run a Mobil Device Management System (MDM) that facilities the ability to provide firewall services from the District;

G. employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the District.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time.

When mobile devices that are authorized for use to access CJI are lost or stolen, the District shall have the ability to determine the location of District controlled smartphones and tablets; and immediately wipe the device.

Personal Firewall

A personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e., laptops or tables with Windows or Linus/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

A. manage program access to the Internet

B. block unsolicited requests to connect to the user device

C. filter incoming traffic by IP address or protocol

D. filter incoming traffic by destination ports

E. maintain an IP traffic log

Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform similar functions a personal firewall would provide on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

Mobile Device Management

If a Mobile Device Management (MDM) is used, the District shall implement the following controls when allowing CJI access from mobile devices, such as mobile phones or smartphones and tablet devices:

A. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.

B. MDM with centralized administration configured and implemented to perform at least the:

1. remote locking of device;

2. remote wiping of device;

3. setting and locking device configuration;

4. detection of "rooted" and "jailbroken" devices;

5. enforcement of folder or disk level encryption;

6. application of mandatory policy settings on the device;

7. detection of unauthorized configurations or software/applications.

Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11x, cellular, Bluetooth, satellite, microwave, and Land Mobile Radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

Wireless Protocols

The District shall implement the following controls for all District-managed wireless access points:

A. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.

B. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.

C. Place APs in secured areas to prevent unauthorized physical access and user manipulation.

D. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.

E. Enable user authentication and encryption mechanisms of the

management interface of the AP.

F. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1

G. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

H. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) of services.

I. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.

J. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.

K. Ensure that the ad hoc mode has been disabled.

L. Disabled all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.

M. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.

N. Insulate, virtually (e.g. Virtual Local Area Network (VLAN) and Access Control Lists (ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.

O. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

Security Training Records

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

A. rules that describe responsibilities and expected behavior with regard to CJI usage

B. implications of noncompliance

C. incident response (Points of contact; Individual actions)

D. media protection

E. visitor control and physical access to spaces - discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity

F. protection of information subject to confidentiality concerns - hardcopy through destruction

G. proper handling and marking of CJI

H. threats, vulnerabilities, and risks associated with handling of CJI

I. social engineering

J. dissemination and destruction

Personnel with Physical and Logical Access

In addition to the above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

A. rules that describe responsibilities and expected behavior with regard to information system usage

B. password usage and management - including creation, frequency of changes, and protection

C. protection from viruses, worms, Trojan horses, and other malicious code

D. unknown e-mail/attachments

E. web usage - allowed versus prohibited; monitoring of user activity

F. Spam

G. physical Security - increases in risks to systems and data

H. media Protection

I. handheld device security issues - address both physical and wireless security issues

J. use of encryption and the transmission of sensitive/confidential information over the Internet - address agency policy, procedures, and technical contact for assistance

K. laptop security - address both physical and information security issues

L. personally owned equipment and software - state whether allowed or not (e.g., copyrights)

M. access control issues - address least privilege and separation of duties

N. individual accountability - explain what this means in the agency

O. use of acknowledgement statements - passwords, access to systems and data, personal use and gain

P. desktop security - discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems

Q. protection of information subject to confidentiality concerns-in systems, archived, on backup media, and until destroyed

R. threats, vulnerabilities, and risks associated with accessing Criminal Justice Information Services (CJIS)

Personnel with Information Technology Roles

In addition to both sets of requirements above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

A. protection from viruses, worms, Trojan horses, and other malicious code - scanning, updating definitions

B. data backup and storage - centralized or decentralized approach

C. timely application of system patches - part of configuration management

D. access control measures

E. network infrastructure protection measures

Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the LASO and provided to MSP as requested or required. A certificate of completion may be provided at the completion of each training. Such certificates shall include the following information: District name, name of employee presented with the proof of completion for undertaking Security Awareness Training, date of completion, authorizing name and title.

Incident Handling and Response

Information system security incidents shall be tracked using Form CJIS-016 and documented on an ongoing basis. Incident-related information may be obtained from audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The LASO shall maintain completed security incident reporting forms for three (3) years or until legal action (if warranted) is complete, whichever timeframe is greater. The District shall ~~prepare and~~ implement ~~a District-specific plan with~~ steps for incident handling capabilities, for both digital and physical CHRI media. At a minimum, the following will be implemented~~The plan must include the following~~:

	Physical – Hard Copy CHRI	Digital – Digitally Saved CHRI
1. Preparation	The CHRI container will be locked at all times in the business office where it is stored. The office must be locked when office staff is not present.	Firewalls, virus protection, and/or malware/spyware protection shall be implemented and maintained to prevent unauthorized access or intrusion of the information systems.

	Physical – Hard Copy CHRI	Digital – Digitally Saved CHRI
2. Detection	Unauthorized activities or physical intrusions to the building shall be monitored by building alarm or video surveillance. Doors must be locked and checked at night.	Electronic intrusions shall be monitored and detected by the firewalls, virus protection, and/or malware/spyware protection software.
3. Analysis	The LASO will work with police authorities to determine how the incident occurred and what data was affected.	The LASO shall work with the IT department to determine what systems or data were compromised and affected.
4. Containment	The LASO will work with police authorities to determine how the incident occurred and what data was affected.	The IT department shall stop the spread of any intrusion of the information systems and prevent further damage.
5. Eradication	The LASO shall work with law enforcement to remove any threats and compromised CHRI data.	The IT department shall remove the intrusion of the information systems before restoring the system. All steps necessary to prevent recurrence shall be taken before restoring the system.

	Physical – Hard Copy CHRI	Digital – Digitally Saved CHRI
6. Recovery	Police shall handle and/or oversee recovery of stolen CHRI media. The LASO may contact MSP for assistance in re-fingerprinting if necessary.	The IT department shall restore the agency information system and media to a safe environment.

~~A. Preparation – Any necessary hardware and/or software implemented to prevent unauthorized access or the intrusion of the information systems (firewalls, virus detection, malware/spyware detection) or locked doors and cabinets to prevent unauthorized physical access.~~

~~B. Detection – A method of preparation and the detailed use of mechanisms (monitoring intrusions such as spyware, worms, or unusual or unauthorized activities or physical intrusions with building alarms or video surveillance).~~

~~C. Containment – The security tools utilized or the plan to stop the spread of the intrusion and prevent any further damage.~~

~~D. Eradication – Removal of the intrusion before the system can be restored and the steps taken to prevent reoccurrence.~~

~~E. Recovery – Steps taken to restore the information system and media to a safe environment (e.g. restore missing files/documents).~~

When an incident involving security of CJI or systems with access to CJI is discovered, the following procedures shall be followed:

A. The LASO shall be notified immediately.

B. The breach shall be assessed and steps taken to correct the situation:

1. Access shall be stopped for any unauthorized user.

2. Media shall be secured.

3. Systems shall be shut down as necessary to avoid further exposure to unauthorized access or dissemination of CJIS.

4. Such other steps as are deemed necessary by the LASO or authorized personnel involved in assessing the incident.

C. All necessary information regarding the security breach and District responses shall be recorded, analyzed, and preserved, including who was involved in taking incident response measures.

D. The LASO shall be responsible for filing the incident report with the MSP.

The LASO shall monitor MSP information/guidance on incident reports and train authorized users with access to CJI on detection and response to security incidents.

Mobile Device – Incident Handling and Response

A. The LASO shall be notified immediately.

B. The breach shall be assessed and steps taken to correct the situation:

1. access shall be stopped immediately, and remotely if necessary, for any authorized user;

2. media shall be secured and steps taken to identify how the incident occurred and what systems or data were compromised or affected;

3. systems shall be shut down as necessary to avoid further exposure to unauthorized access or dissemination of CJIS;

4. such other steps as are deemed necessary by the LASO or authorized personnel involved in assessing the incident.

C. All necessary information regarding the security breach and District responses shall be recorded, analyzed, and preserved, including who was involved in taking incident response measures.

D. Steps shall be taken to restore the devise and media to a safe environment.

E. The LASO shall be responsible for filing the incident report with the MSP using form CJIS-016. A copy of the completed form shall be retained and produced to MSP upon request.

When a device is lost the District shall document and indicate how long the device has been lost. Special reporting procedures for mobile devices shall apply in any of the following situations:

A. for a lost device, report if the owner:

1. believed the device was locked

2. believed the device was unlocked

3. could not validate the device's locked state

B. for a total loss of a device, report if:

1. CHRI was stored on the device

2. the device was locked or unlocked

3. capable of remote tracking or wiping of device

C. report any compromise of a device when the intrusion occurs while still in the owner's possession

D. report any compromise outside of the United States

Collection of Evidence

Where an information security incident involves legal action against the District or an individual (either civil or criminal), evidence shall be collected, retained, and presented in accordance with the rules of evidence of the relevant jurisdiction(s).