

Vol. 41, No. 1 - September 2026 Revised CRIMINAL JUSTICE INFORMATION SECURITY (Non-Criminal Justice Agency)

ADOPTED Apr 19, 2024

8321 - 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 annually, or when there is evidence of authenticator compromise ~~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 annually, or when there is evidence of authenticator compromise ~~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 as follows which have the following characteristics :

1. Maintain a list of commonly-used, expected, or compromised passwords; update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly; and compare current passwords against the list quarterly ~~The password contains less than eight (8) characters~~ .
2. When processing requests to establish or change passwords, compare prospective passwords against the list described above ~~The password is a word found in a dictionary (English or foreign)~~ .
3. If a chosen password is found in the list, the verifier shall advise the subscriber that a different password is required, provide the reason for rejection, and require the subscriber to choose a different password. ~~The password is a common usage word such as :~~
 - a. Verifiers shall not prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing passwords ~~names of family, pets, friends, co-workers, fantasy characters, etc.~~
 - b. Password verifiers shall not permit the subscriber to store a password hint that is accessible to an unauthenticated user. ~~computer terms and names, commands, sites, companies, hardware, software~~
 - c. Verifiers shall implement a rate-limiting mechanism that limits failed authentication attempts on a subscriber's account to no more than five (5) attempts. ~~the words District, WVSP, HPD, CKSFP or any derivation~~

- d. Verifiers shall force a change of password if there is evidence of compromise of the authenticator ~~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., secret1, lsecret)~~

B. Use strong passwords as follows ~~which have the following characteristics~~ :

1. Allow users to select long passwords and passphrases, including spaces and all printable characters. ~~contain both upper and lower case characters (e.g., a-z, A-Z)~~
2. Passwords chosen by the subscriber shall be at least eight (8) characters in length. ~~have digits and punctuation characters as well as letters, e.g., 0-9. !@#\$\$%^&()_+{}[];:<>?,.?~~
3. Passwords shall not be truncated. ~~are at least eight (8) alphanumeric characters long~~
4. Password verifiers shall store passwords in a form resistant to offline attacks and shall salt and hash them using a suitable one-way key derivation function. ~~are not a word within any language, slang, dialect, jargon, etc.~~
5. The verifier shall use approved encryption when requesting passwords to provide resistance to eavesdropping and MitM attacks. ~~are not based on personal information, names of family, etc.~~
6. The verifier shall use an authenticated protected channel when requesting passwords to provide resistance to eavesdropping and MitM attacks. ~~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 Tmb1W>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 their ~~his/her~~ immediate supervisor.
- B. Contractor should inform their ~~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 256 bit strength ~~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 140-3 standards. FIPS 140-2 certificates will not be acceptable after September 21, 2026 standards.
 - 1. Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-3 compliance ~~140-2-compliance~~ can be used in the interim until certification is complete.
 - 2. Note 2: While FIPS 197 (Advanced Encryption Standard) certification with a symmetric cipher key of at least 256 bit strength is required ~~desirable~~, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-3 ~~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 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 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 Mobile Device Management System (MDM) that facilitates 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 tablets with Windows or Linux/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) system 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. Disable 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

Role-based security and privacy training shall be provided to personnel with the following roles and responsibilities before authorizing access to the system, information, or performing assigned duties, annually thereafter, and when required by system changes. ~~At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJIT:~~

NOTE: The CSO/SIB Chief may accept documentation of the completion of role-based security and privacy training from another agency. Accepting such documentation means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by Federal, State, or local laws.

Role-based training content shall be updated annually and following audits of the CSA and local agencies, changes in the information system operating environment, security incidents, or changes to the CJIS Security Policy.

All individuals with unescorted access to a physically secure location

- A. ~~rules that describe responsibilities and expected behavior with regard to CJIT usage~~
- B. ~~implications of noncompliance~~
- C. ~~incident response (Points of contact; Individual actions)~~
- D. Section 4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information
Penalties ~~media protection~~
- E. IR-2 Incident Response Training ~~visitor control and physical access to spaces - discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity~~

- F. IR-6 Incident Reporting protection of information subject to confidentiality concerns -
hardcopy through destruction
- G. PE-2 Physical Access Authorizations proper handling and marking of CJJ
- H. PE-3 Physical Access Control threats, vulnerabilities, and risks associated with handling of
CJJ
- I. PE-6 Monitoring Physical Access social engineering
- J. PE-8 Visitor Access Records dissemination and destruction
- K. PS-8 Personnel Sanctions

General User Personnel with Physical and Logical Access

A user, but not a process, who is authorized to use an information system. In addition to the topics identified above, the following topics shall be included: , at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJJ:

- A. Section 4.1 Criminal Justice Information rules that describe responsibilities and expected behavior with regard to information system usage
- B. Section 4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information password usage and management - including creation, frequency of changes, and protection
- C. Section 4.3 Personally Identifiable Information protection from viruses, worms, Trojan horses, and other malicious code
- D. AC-3 Access Enforcement unknown e-mail/attachments
- E. AC-6 Least Privilege web usage - allowed versus prohibited; monitoring of user activity
- F. AC-8 System Use Notification Spam
- G. AC-11 Device Lock physical Security - increases in risks to systems and data
- H. AC-18 Wireless Access media Protection
- I. AC-20 Use of External Systems handheld device security issues - address both physical and wireless security issues

- J. AT-2(3) Literacy Training and Awareness/Social Engineering and Mining use of encryption and the transmission of sensitive/confidential information over the Internet - address agency policy, procedures, and technical contact for assistance
- K. AU-6 Audit Record Review, Analysis, and Reporting laptop security - address both physical and information security issues
- L. CA-3 Information Exchange personally owned equipment and software - state whether allowed or not (e.g., copyrights)
- M. IA-2 Identification and Authentication (Organizational Users) access control issues - address least privilege and separation of duties
- N. IA-5(1)(a) Memorized Secret Authenticators and Verifiers individual accountability - explain what this means in the agency
- O. MP Media Protection use of acknowledgement statements - passwords, access to systems and data, personal use and gain
- P. MP-2 Media Access desktop security - discuss use of screensavers, restricting visitors' view of information on screen (mitigating shoulder surfing), battery backup devices, allowed access to systems
- Q. MP-4 Media Storage protection of information subject to confidentiality concerns in systems, archived, on backup media, and until destroyed
- R. PE-5 Access Control for Output Devices threats, vulnerabilities, and risks associated with accessing Criminal Justice Information Services (CJIS)
- S. SC-13 Cryptographic Protection
- T. SC-28 Protection of Information at Rest
- U. SI-3/5.20.4.2 Malicious Code Protection
- V. SI-8 Spam Protection
- W. Section 5.20.1.2 Cellular Devices
- X. Section 5.20.2 Mobile Device Management

Privileged User

A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform. In addition to the topics identified above, the following topics shall be included:

1. AC Access Control
2. CP-6 Alternate Storage Site
3. CP-9 System Backup
4. SC System and Communications Protection
5. SI-2 Flaw Remediation
6. Most recent changes to the CJIS Security Policy

Organizational Personnel with Security Responsibilities

Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJIS Security Policy. In addition to the topics identified above, the following topics shall be included:

1. Section 3.2.9 Organizational Personnel with Information Security Responsibilities
2. Authorized Recipient Security Officer Role

3. Additional State/local/tribal/territorial or Federal agency roles and responsibilities
4. Summary of audit findings from previous State audits of local agencies
5. Findings from the last FBI CJIS Division audit

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.

Auditing and Accountability (CHRI Digital Storage)

The District's information system shall generate audit records ~~record~~ for the events listed below. The District shall specify which information system component shall carry out auditing activities.

The District's information system shall produce, at the application and/or operating system level audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events, in the event the District does not use an automated system, manual recording of activities shall still take place.

The following event types shall be logged:

- A. All successful and unsuccessful system log-on attempts.
- B. All successful and unsuccessful attempts to use, access, create, write, delete, or change permissions on user accounts, files, directories, or other system resources.
1. ~~access permission on a user account, file, directory or other system resource;~~
 2. ~~create permission on a user account, file, directory or other system resource;~~
 3. ~~write permission on a user account, file, directory or other system resource;~~
 4. ~~delete permission on a user account, file, directory or other system resource;~~
 5. ~~change permission on a user account, file, directory or other system resource.~~

All successful ~~Successful~~ and unsuccessful attempts to change account passwords.

All successful ~~Successful~~ and unsuccessful actions by privileged accounts.

All successful ~~Successful~~ and unsuccessful attempts ~~by~~ for users to access, modify, or destroy the audit log file.

- A. ~~access the audit log file;~~
- B. ~~modify the audit log file;~~
- C. ~~destroy the audit log file.~~

The following content shall be included with every audited event: (a) what type of event occurred; (b) when the event occurred; (c) where the event occurred; (d) the source of the event; (e) the outcome of the event; and (f) the identity of any individuals, subjects, or objects/entities associated with the event ~~1) date and time of the event; 2) the component of the information system (e.g., software component, hardware component) where the event occurred; 3) type of event; 4) user identity; and 5) outcome (success or failure) of the event.~~

The District's information system shall alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour ~~provide alerts to the appropriate District officials~~ in the event of an audit logging process ~~processing~~ failure and shall take the following additional actions: restart all audit logging processes and verify that the system(s) is/are logging properly. Audit logging process ~~processing~~ failures include, for example software and hardware ~~software/hardware~~ errors, failures in the audit log capturing mechanisms, and audit log storage capacity being reached or exceeded.

Audit Monitoring, Analysis, and Reporting – The District shall designate an individual or position to review and analyze ~~review/analyze~~ information system audit records for indications

of inappropriate or unusual activity and the potential impact of such activity, to investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit record review, analysis, and reporting ~~review/analysis~~ shall be conducted weekly, and the level of review, analysis, and reporting shall be adjusted when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information ~~at a minimum once a week, and should be increased if volume indicates an elevated need for audit review~~.

Time Stamps – The District’s information system shall use internal system clocks to generate ~~provide~~ time stamps for use in audit records ~~ecord-generation~~. The time stamps shall meet hundredths of a second (i.e., hh:mm:ss:00) interval and shall use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or include the local time offset as part of the time stamp ~~include the date and time values generated by the internal system clocks in the audit records~~.

Protection of Audit Information – The District’s information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

Audit Record Retention – The District shall retain audit records for a minimum of ~~at least~~ one (1) year or ~~Once the minimum retention time period has passed, the District may continue to retain audit records~~ until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.

© Neola 20 ~~26~~ ~~21~~