#15: CJIS Security Policy

I. PURPOSE

The purpose of this Policy is to ensure the security, confidentiality, integrity, and availability Criminal Justice Information (CJI), accessed, processed, stored, or transmitted by Cumberland County systems. This Policy establishes requirements in accordance with the FBI Criminal Justice Information Services (CJIS) Security Policy, Maine Electronic Telecommunications & Routing Operations (METRO) Manual, and other applicable state and federal regulations and policies.

This Policy applies to all County-owned or managed information systems and all physical locations where CJI is accessed or stored. All Cumberland County officials, employees, contractors, vendors, and partners with access to CJIS information in Cumberland County information systems and physical locations, shall abide by the policies and procedures set forth in this Policy, the Maine METRO manual and the federal CJIS Security Policy.

II. DEFINITIONS

AIU – Access Integrity Unit, division of the Maine State Police which provides access, support and training of the METRO, NLETS, and NCIC systems.

CJI- Criminal Justice Information, the data necessary for criminal justice agencies to perform their mission and enforce the laws.

CJIS – Criminal Justice Information Services, division of the FBI which provides access to National Crime Information Center (NCIC) and other nationwide criminal justice information.

CCIS- Cumberland County Information System, any media or area owned or maintained by Cumberland County that processes, stores, or transmits CJI. CCIS includes the following:

1. Digital media: any electronic storage media, including internal hard drives, solid-state drives, external hard drives, USB flash drives, optical disks (CDs/DVDs), backup tapes, and memory cards.
2. Physical Media: any non-digital medium where CJI is recorded, including but not limited to paper printouts, microfilm, microfiche, and printer/fax ribbons.
3. Controlled Area: A space, room, or facility where access is physically or procedurally controlled to protect information and systems.

LASO – Local Area Security Officer, security liaison with the Maine State Police, CJIS Systems Agency and Information Security Officer.

METRO – ME Telecommunications and Routing Operations system, State network which facilitates the exchange of criminal justice information and messages.

TAC – Terminal Agency Coordinator, information access liaison with the AIU.

III. SECURITY AND AWRENESS TRAINING POLICY

A. Training. All individuals who have access to CCIS shall complete security awareness training.

A. Training shall be completed prior to granting initial access CCIS. Training shall be completed at least annually thereafter. Training shall be provided more frequently if system changes are implemented and for individuals involved in a security event.

B. Mandatory topics for basic security awareness training include:

A. Training on recognizing and reporting potential indicators of insider threat.

B. Training on recognizing and reporting potential and actual instances of social engineering and social mining.

C. Procedures for handling personally identifiable information (PII).

C. Security training shall be role-based as follows:

A. **Individuals with Unescorted Access (Level 1)**- individuals with physical access to secure areas, but no logical access to information systems, (i.e., custodial staff and vendors) shall receive training on the following topics:

i. Penalties for improper access, use, dissemination of CJI.

ii. Reporting Security Events.

iii. Incident Response Training.

iv. System Use Notification.

v. Physical Access Authorizations and Controls.

vi. Monitoring Physical Access.

vii. Visitor Control.

viii. Personnel Sanctions.

B. **General Users (Level 2)**- all individuals with logical access to systems processing CJI (i.e., Patrol Officers (CCSO), Dispatchers, etc.) shall receive training on the following topics:

i. All topics required for Level 1.

ii. Proper Access, Use, and Dissemination of CJI and NCIC Non-Restricted Files.

iii. Handling Personally Identifiable Information (PII).

iv. Media Protection (Storage, Access, Sanitization).

v. Password management and usage.

vi. Social Engineering and Phishing detection.

vii. Malicious Code Protection.

viii. Mobile Device Security (if applicable).

ix. Wireless Device Risk Mitigations.

x. Encryption requirements.

C. **Privileged Users (Level 3)**- individuals with elevated permissions to use or modify information systems (i.e., account managers, supervisors) shall receive training on the following topics:

i. All topics required for Levels 1 and 2.

ii. Access Control Mechanisms.

iii. System and Communications Protection.

iv. Patch Management.

v. Audit trail responsibilities.

vi. Backup and storage procedures (centralized/decentralized).

vii. Most recent changes to the CJIS Security Policy.

D. **Security Managers (Level 4)**- individuals responsible for security management of County information systems and personnel (i.e., LASO, TAC, IT Director, etc.) shall receive training on the following topics:

i. All topics required for Levels 1, 2, and 3.

ii. Local Agency Security Officer (LASO) Role responsibilities.

iii. Authorized Recipient Security Officer Role.

iv. Applicable State/Federal agency roles.

D. Documentation of current security awareness training for all personnel must will be kept on file for a minimum of three (3) years. Records must include the name of the trainee, date of training, content/type of training provided, and verification of completion.

IV. INCIDENT RESPONSE

A. Incident Response Plan

a. The County IT Director shall develop, document, and disseminate the County's Incident Response Plan (IRP) and its supporting procedures to all personnel with incident response responsibilities. The IRP shall define reportable incidents and provide a roadmap for response, including preparation, detection, containment, eradication, and recovery procedures.

b. Individuals subject to this Policy are required to report any suspected incident involving CJI or CCIS to the IT HelpDesk immediately- not to exceed one (1) hour.

1. A "suspected incident" includes, but is not limited to: receipt of a suspicious email (phishing); a virus or malware alert on a workstation; unusual system behavior or pop-up messages; loss or theft of any County-issued device (laptop, phone) or media (USB drive); any unauthorized access to a file, system, or secure area.

2. Any confirmed security incident will be reported to the AIU.

c. The IRP shall be protected for unauthorized disclosure, reviewed, annual, and updated following any significant incident.

B. Incident Response Training

a. Any individual with access to CJI shall obtain role-based Incident Response Training as discussed in the Training Section of this Policy.

C. Testing

a. The IRP shall be tested at least every two years (i.e., via table top exercise or simulations) to determine its effectiveness and the County's readiness.

b. Testing shall be coordinated with other related plans (i.e., Contingency Plan, Disaster Recovery Plans, etc.).

D. Response Assistance

a. The County IT Department (Help Desk) shall serve as the primary 24/7 incident response support resource, offering advice and assistance to all personnel for handling and reporting suspected incidents.

V. AUDITING AND ACCOUNTABILITY

A. The County IT Department shall maintain a log of all log-on and log-off attempts, all account changes, and privileged activity.

a. Logs shall be maintained for a minimum of one (1) year and logs for activity occurring within the past 90 days must be immediately accessible.

b. Logs must be stored in a manner that prevents unauthorized or accidental modification.

B. The County shall conduct periodic risk assessments, identify threats, vulnerabilities and their impacts, and document and track risk mitigation decisions.

VI. ACCESS CONTROL POLICY

A. In General. Access to CJI in a CCIS is restricted to authorized users for official criminal justice purposes only. Access shall follow the principle of least privilege.

B. Access Enforcement/Least Privilege. All County officials, employees, contractors, vendors, and individuals responsible for overseeing access to the County CJI shall:

a. Employ the principle of least privilege, allowing only authorized accesses to CJI for users that are necessary to accomplish assigned tasks in accordance with the County's operations and goals. Access authorizations (i.e., file permissions, application roles, etc.) shall be strictly enforced to align with this principle.

b. Require users of information system accounts use separate, non-privileged accounts when accessing all standard, non-CJI related functions.

c. Ensure CCIS audits the execution of privileged functions.

d. Ensure CCIS prevents non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards and countermeasures.

C. Account Management.

a. The County IT Department shall:

i. Maintain account inventories and access levels to CJI stored in County digital media.

ii. Disable digital accounts as follows:

1. Inactive accounts after 90 calendar days.

2. Accounts for any person who is terminated, transferred, or no longer requires access to CJI within 24 hours of the status change.
3. High-risk accounts, or accounts identified as a direct threat to CJI within thirty (30) minutes of discovery.
4. Temporary and emergency accounts after usage.

iii. Ensure that the County digital CCIS automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate personnel.

b. Each department shall assign a LASO who shall:

i. Provide the County IT Department with a list of individuals in their department and/or working with their department who are authorized to access CJI and the individual's level of access.

ii. Notify the IT Department when digital accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.

iii. Review all user accounts and access privileges at least annually for compliance with account management requirements.

D. System Use Notification. The County IT Department shall ensure that all digital information systems providing access to CJI display an approved system use notification message or banner to users before granting access to the system.

a. This message shall state that:

i. Users are accessing a restricted County information system.

ii. System usage may be monitored, recorded, and subject to audit.

iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

iv. Use of the information system indicates consent to monitoring and recording

v. There are no rights to privacy.

b. The message shall be retained on the screen until the user acknowledges the usage conditions and take explicit actions to log on to further access the information system.

E. Session Management. The County IT Department shall ensure:

a. Any user account or device with access to CJI shall be automatically locked after five (5) consecutive invalid logon attempts within a fifteen (15) minute period. The account must remain locked until released by an administrator.

b. All devices used to access CJI shall employ a device lock that automatically activates after a maximum of thirty (30) minutes of inactivity. The user must re-authenticate to re-establish access.

c. Users must log out of the information system when their work period is complete. Sessions shall be configured to terminate automatically after logout.

d. Information previously visible must be concealed when the session is locked with a publicly visible image or display.

F. Remote, Mobile, and Wireless Access.

a. All users requiring remote or wireless access to CCIS must be authorized by the Department's LASO. All remote and wireless access must be documented and monitored.

b. All remote and wireless access sessions transmitting CJI must be protected using cryptographic mechanisms compliant with FIPS 140-2 (i.e., an approved VPN solution).

c. Only County issued or controlled mobile devices (i.e., laptops, tables, smartphones, etc.) are authorized to access or store CJI.

d. All authorized mobile devices used to access CJI must be protected by full-device or container-based encryption compliant with FIPS 140-2.

G. External Systems and Information Sharing.

a. The use of external information systems, including personally-owned devices and publicly accessible systems (i.e., hotels or library computers) to access, process, store, or transmit CJI is strictly prohibited.

b. The sharing of CJI with any external agency or individual is prohibited, unless done in accordance with state and federal law and an approved Information Exchange Agreement.

VII. IDENTIFICATION AND AUTHENTICATION

A. User Identification.

a. All users shall be issued a unique username for their exclusive use to access CJI. This identifier must be traceable to a specific, known individual.

b. The use of shared or group accounts is prohibited for individual users. Shared accounts may only be used for system process or functions where individual accountability is otherwise maintained through logs or other means, and must be approved by the IT Director or system manager.

B. Identity Proofing.

a. All County personnel requiring access to CJI must undergo identity proofing that meets or exceeds the requirements for **Identity Assurance Level 2 (IAL2)** as defined in NIST SP 800-63A.

b. Identity proofing must include the collection, validation, and verification of official identity evidence (i.e., government-issued ID). This process must be completed in person by an authorized County representative or via an approved and secure remote identify proofing process before access is granted.

C. Multi-Factor Authentication

a. Multi-Factor Authentication (MFA) is mandatory for all logical access to any information system that stores, processes, or transmits CJI. This applies to all access, including but not limited to:

1. Remote access (e.g., VPN, web portals).

2. On-premises (internal network) access.
3. Access to privileged (administrator) accounts.
4. Access to non-privileged (standard user) accounts.

b. All authentication mechanisms must meet or exceed the requirements for Authenticator Assurance Level 2 (AAL2) as defined in NIST SP 800-63B.

c. AAL2 requires the use of two distinct authentication factors from the following categories:

1. Something You Know: A memorized secret (e.g., password, PIN).
2. Something You Have: A physical authenticator (e.g., a hardware token, a PIV/smart card, a mobile device using an approved authenticator app).
3. Something You Are: A biometric (e.g., fingerprint, iris scan).

d. Using two of the same type of factors (e.g., a password and a PIN) is not MFA and is not permitted.

D. Password Management

a. Passwords used to access CJI, including access directly to the CCIS must meet the following requirements:

1. Contain a minimum of eight (8) characters.
2. Cannot be a dictionary word or proper name.
3. Cannot be the same as the username.
4. Must be changed every ninety (90) days.
5. The system shall prevent reuse of the last ten (10) passwords.
6. Passwords shall not be transmitted in clear text outside the secure network.

b. Passwords must be changed immediately if there is any evidence or suspicion that the authenticator has been compromised

c. All passwords must be stored in a salted and hashed format using a one-way, FIPS-validated key derivation function. Passwords shall never be stored in plain text or in a reversibly encrypted format.

1. The County IT Department shall establish and maintain secure procedures for the full lifecycle of all physical authenticators including:
    a. Secure issuance and binding to a user's verified identity.
    b. Maintaining an inventory of all issued authenticators.
    c. Immediately revoking authenticators that are lost, stolen, compromised, or associated with a terminated user.
    d. Securely destroying expired or revoked physical authenticators.

E. Identifier and Device Management

a. LASOs must immediately notify the IT Department of any personnel transfer, separation, or change in access requirements to the CCIS. The IT Department must ensure that all system access is terminated upon notification.

b. Disabled user identifiers shall not be re-issued to another individual user for a minimum of one (1) year after the user's separation from the County.

c. All devices (including workstations, mobile devices, and servers) must be uniquely identified and authenticated before being granted access to CJI (e.g., via 802.1x, device certificates, or MAC address validation). All information systems shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

VIII. CONFIGURATION MANAGEMENT

A. The County shall:

a. Maintain baseline system configurations.

b. Implement formal change control procedures.

c. Preform security impact analysis before changes.

d. Track and document all system modifications.

IX. MEDIA PROTECTION

A. Media Storage and Access

a. All digital and physical media containing CJI shall be securely stored within a physically secure location or a controlled area. When not in active use, media must be stored in a locked drawer, cabinet, safe, or room.

b. Media containing CJI (e.g., printouts, laptops, external drives) shall not be left unattended or in plain view in an unsecured area. Precautions must be taken to obscure CJI from public or unauthorized view.

B. Media Transport

a. Physical Media Transport: Physical media (e.g., paper files) shall be placed in an opaque, sealed envelope or a locked container to prevent viewing during transport.

1. Hand-carried media shall be under the direct, physical control of the authorized personnel at all times.

b. Digital Media Transport: All CJI stored on digital media (e.g., laptops, USB drives) must be encrypted using a FIPS 140-2 validated cryptographic module before the media is transported.

1. If encryption is not feasible for a specific legacy device, the device must be transported by authorized personnel in a locked, secure container.

c. Shipment: Any media shipped via mail or courier must use a service that provides shipment tracking and requires a signature upon delivery. The media must be securely packaged and, if digital, must be encrypted.

C. **Media Sanitization and Disposal.** Any electronic media used to store CJIS information that is to be reused for non-CJI information will be turned over to the County IT Department to be sanitized prior to being reused.

a. All media must be properly sanitized or destroyed prior to disposal, release from County control, or release for reuse in a less secure capacity. Sanitization and disposal methods shall be consistent with NIST SP 800-88 (Guidelines for Media Sanitization).

b. **Digital Media Sanitization:** Digital media shall be sanitized by overwriting the data at least three (3) times or using a method that meets or exceeds the NIST "Clear" or "Purge" standard. Magnetic media (e.g., HDDs, tapes) may be sanitized by degaussing with an approved degausser that is rated for the media's coercivity. Media that cannot be sanitized (e.g., inoperable drives, SSDs, CDs/DVDs) or media that has reached its end-of-life shall be physically destroyed by shredding, disintegrating, pulverizing, or incinerating.

c. **Physical Media Disposal:** All physical media (e.g., paper, printer ribbons) containing CJI shall be securely disposed of when no longer required. Disposal must be accomplished by cross-cut shredding or incineration to a particle size that renders the information unrecoverable.

d. **Documentation and Witnessing:** All sanitization and destruction of media shall be witnessed or carried out by authorized personnel. A permanent record (e.g., "Certificate of Sanitization/Destruction") shall be maintained by the LASO or County IT Department, documenting the media type, serial number (if applicable), sanitization method, date, and the authorized personnel who performed and/or witnessed the action.

D. **Media Use and Marking**

a. Use of publicly accessible computers (e.g., in hotels, libraries, business centers) or personally-owned media (e.g., personal USB drives) to access, process, store, or transmit CJI is prohibited.

b. All media containing CJI that is transported outside a controlled area shall be clearly marked to indicate its sensitivity and handling requirements.

X. PHYSICIAL AND ENVIRONMENTAL PROTECTION POLICY

A. **Physical Access Authorizations.** Each LASO, working with the County IT Department and Facilities Department shall:

a. Maintain a documented list of all individuals with authorized access to facilities and secure areas where CJI information is stored.

b. Issue authorization credentials (i.e., key cards, access badges) to all individuals with authorized access.

c. Review and validate access lists at least annually and upon any transfer or termination or changes to individual access privileges.

d. Revoke access for individuals no longer requiring it (i.e., due to termination, transfer, or change in duties) and retrieve physical access credentials.

B. **Physical Access Controls.** Each LASO, working with the County IT Department and Facilities Department shall:

a. Enforce physical access authorizations at all entry and exit points to secure facilities and areas. Access shall be verified before granting entry.

b. Require all visitors to secure areas to be escorted by authorized personnel at all times.

c. Maintain a log of all visitor activity into secure areas.

d. Securely manage all keys, combinations, and other physical access devices. Combinations and keys shall be changed when keys are lost, combinations are compromised, or when individuals with knowledge of them are terminated or transferred.

e. Maintain and review physical access logs for secure locations quarterly.

C. Access Control for Output Devices

a. Physical access to CCIS output devices (e.g., printers, copiers, fax machines, monitors) shall be controlled to prevent unauthorized individuals from obtaining sensitive information.

1. Output devices shall be placed in secure, monitored locations.
2. Printed CJI shall be retrieved immediately by the authorized user.
3. Monitors displaying CJI shall be positioned to prevent unauthorized viewing.

D. Monitoring Physical Access

a. Physical access to all secure facilities and areas containing CJI shall be monitored 24/7 to detect and respond to physical security incidents.

b. Monitoring shall be conducted using physical intrusion alarms and/or surveillance equipment (e.g., video cameras).

c. Physical access logs and surveillance records shall be reviewed at least quarterly by the LASO and upon any security incident.

d. Results of reviews and investigations shall be coordinated with the County's incident response policy.

E. Visitor Access Records

a. LASOs shall maintain visitor access records for all entries to secure facilities for a minimum of one (1) year.

b. Visitor access records shall be reviewed at least quarterly to identify any anomalies.

c. Logs shall contain sufficient information to identify the visitor, their organization, the date/time of access, purpose of visit, and the name of the personnel visited/escort.

F. Power Equipment and Cabling

a. All power equipment and cabling for information systems in secure areas (e.g., data centers, server rooms) shall be protected from damage and destruction.

G. Emergency Shutoff

a. Data centers and server rooms shall be equipped with emergency shutoff switches for power.

b. These switches shall be placed in easily accessible locations for authorized emergency personnel.

c. Emergency shutoff switches shall be protected from unauthorized activation.

H. Emergency Power

a. An uninterruptible power supply (UPS) and/or backup generator shall be provided for critical information systems to facilitate an orderly shutdown or transition to alternate power in the event of a primary power source loss.

I. Emergency Lighting

a. Automatic emergency lighting shall be employed and maintained for all secure facilities, covering emergency exits and evacuation routes, to activate in the event of a power outage.

J. Fire Protection

a. Fire detection and suppression systems (e.g., smoke detectors, sprinklers, fire extinguishers) shall be employed and maintained in all secure facilities, especially data centers and server rooms.

b. Detection and suppression systems shall be supported by an independent energy source.

c. Detection systems shall be configured to activate automatically and notify emergency responders and appropriate County personnel.

K. Environmental Controls

a. Temperature and humidity (HVAC) levels within data centers and server rooms shall be maintained at acceptable levels as defined by equipment manufacturers and industry best practices. These levels shall be monitored.

L. Water Damage Protection

a. Data centers and server rooms shall be protected from water damage (e.g., from plumbing, leaks). Master shutoff or isolation valves for water sources shall be accessible to key personnel.

M. Delivery and Removal

a. The County shall authorize, control, and maintain records for all information system components entering and exiting the facility to protect against theft or the introduction of unauthorized hardware.

N. Alternate Work Site

a. All alternate work sites (e.g., telework locations, employee residences) used to access, process, store, or transmit CJI must be formally documented and approved.

b. Personnel operating from an alternate work site shall adhere to the following controls:

1. Officials, employees, contractors, vendors, and any other individual with access to CJI must ensure their work area is secured to prevent unauthorized individuals (including family members or visitors) from accessing or viewing CJI.

2. All electronic CJI must be encrypted at rest in accordance with the CJIS Security Policy.
3. Physical copies of CJI are not to be printed at alternate work sites.
4. Users shall lock their session or device when leaving the area unattended.
5. A means for employees to communicate with County security personnel in case of an incident shall be provided.

XI. SYSTEM AND COMMUNICATIONS PROTECTION

A. All CJI transmitted outside secure networks must use FIPS 140-2 validated encryption.

B. Network protections shall include; firewalls, IDS/IPS, and secure VPN access.

XII. SYSTEM AND INFORMATION INTEGRITY POLICY

A. Flaw Remediation (Patch Management)

a. The County IT Department shall promptly identify, report, and correct system flaws.

b. All software and firmware updates (patches) related to flaw remediation shall be tested for effectiveness and potential side effects on a non-production system before being installed on operational systems.

c. Security-relevant software and firmware updates shall be installed within the following timeframes based on the vulnerability's assessed risk level:

1. **Critical:** 15 days from release.
2. **High:** 30 days from release.
3. **Medium:** 60 days from release.
4. **Low:** 90 days from release.

d. All flaw remediation activities shall be incorporated into the County's configuration management process.

B. Malicious Code Protection

a. The County IT Department shall implement signature-based malicious code (e.g., virus, worm, Trojan horse, spyware) protection mechanisms at key system entry and exit points (e.g., firewalls, email servers, web servers, workstations).

b. Malicious code protection mechanisms shall be configured to automatically update signatures and detection engines as new releases are available.

c. Protection mechanisms shall be configured to:

1. Perform periodic scans of the system at least **daily**.
2. Perform **real-time scans** of files from external sources (e.g., email attachments, web downloads) as they are downloaded, opened, or executed.

d. Malicious code shall be blocked or quarantined upon detection. The IT Department shall be alerted, and incident response procedures (as defined in the IR Policy) shall be implemented.

C. System Monitoring

a. The County IT Department shall monitor the County's information systems to detect attacks, indicators of potential attacks, and unauthorized local, network, or remote connections.

b. Monitoring shall be achieved through tools such as intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM) systems, and firewall logs.

c. Detected events and anomalies shall be analyzed by authorized IT and security personnel to determine if an incident has occurred.

d. The level of system monitoring shall be adjusted based on changes in risk, threat intelligence, or upon discovery of a new vulnerability.

D. Security Alerts and Advisories

a. The County IT Department shall receive security alerts, advisories, and directives from official external sources (e.g., Cybersecurity and Infrastructure Security Agency (CISA), US-CERT, Multi-State Information Sharing & Analysis Center (MS-ISAC), and hardware/software vendors).

b. Internal security alerts and advisories shall be generated and disseminated to all relevant County personnel, administrators, and system owners.

c. The County shall implement mandatory security directives in accordance with their established timeframes.

E. Software, Firmware, and Information Integrity

a. The County IT Department shall employ integrity verification tools and processes (e.g., file integrity monitoring, cryptographic hashes) to detect unauthorized changes to County software, firmware, and information systems that contain or process CJI.

b. Upon the detection of an unauthorized change, the County's Incident Response Plan shall be followed.

F. Spam Protection

a. The County IT Department shall employ spam protection mechanisms (e.g., email filtering) at system entry and exit points to detect and act on unsolicited messages.

b. Spam protection mechanisms shall be updated automatically when new releases and definitions are available.

G. Information Input Validation

a. The County IT Department shall ensure that all information inputs are checked for validity to protect against malicious content and attacks (e.g., SQL injection, cross-site scripting). This control must apply to all inputs to web applications, database servers, and any system component that receives or processes CJI or other sensitive data from an external source.

H. Error Handling

a. System-generated error messages shall be configured to provide information necessary for corrective action without revealing sensitive or potentially exploitable information (e.g., system stack traces, database structures, account information).

b. Detailed error messages shall only be revealed to authorized IT and administrative personnel.

I. Information Management and Retention

a. All County information, including CJI, shall be managed and retained in accordance with applicable federal, state, and local laws, regulations, and established retention schedules.

b. Information that has exceeded its required retention period shall be disposed of in accordance with the County's policies governing media protection and applicable state record retention requirements.

J. Memory Protection

a. To protect against sophisticated malware and exploits, County information systems shall implement memory protection controls where technically feasible. This includes, but is not limited to: Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR)

XIII. PERSONNEL SECURITY

A. All personnel will be identified by a unique user name to be used when accessing the CJIS network.

B. All personnel with logical or direct access to CJIS information will undergo a fingerprint-based background check within thirty (30) days of employment. Outside agencies that access CJIS information through the County will be responsible for performing fingerprint-based background checks on their employees and providing this information to the County.

C. Upon separation of employment, Human Resources or the appropriate agency official will notify the County's Information Technology Department, who will disable the employee's user account.

XIV. SYSTEM AND SERVICES ACQUISITION POLICY

A. Vendors handling CJI must meet CJIS requirements and sign a CJIS Security Addendum.

B. Cloud providers with access to, using, or maintaining CJI through CCIS must be CJIS-compliant.

XIV. ENFORCEMENT

Any individual found to have violated this Policy may be subject to disciplinary actions, including termination under the County's personnel policies, and/or criminal prosecution pursuant to applicable State and Federal laws.

EFFECTIVE DATE: June 15th, 2026