MINNESOTA DEPARTMENT OF NATURAL RESOURCES

DIVISION OF ENFORCEMENT

DIRECTIVE

DIRECTIVE NUMBER: A-30-24

SUBJECT: DIGITAL, PHYSICAL, AND ENVIRONMENTAL CJIS DATA PROTECTION

EFFECTIVE DATE: 12/20/2024

SPECIAL INSTRUCTIONS: CJIS Model Policy

APPENDIX: None

REFERENCE: National Institute of Standards and Technology (NIST); FBI CJIS Security Policy,

DISTRIBUTION: All Division Staff

NUMBER OF PAGES: 5

This directive is for division use only and does not modify or supersede any law and should not apply to any criminal or civil proceeding except for civil proceedings related to departmental administrative actions. This directive should not be viewed as creating a higher standard of safety or care in any evidentiary sense. Violations of this directive may form the basis for departmental administrative action.

I. PURPOSE

To ensure Information Technology (IT) resources and media are protected by physical and environmental security measures to prevent physical tampering, damage, theft, or unauthorized physical access.

II. POLICY

This policy applies to all users of IT resources and assets of the division.

III. DEFINITIONS

A. CJI: Criminal Justice Information

B. LASO: Local area security officer. Staff assigned network security duties designated by the Bureau of Criminal Apprehension (BCA).

IV. PHYSICAL ACCESS RESPONSIBILITIES

A. Physical Access Authorizations.

1. Develop, approve, and maintain a list of individuals with authorized access to locations where the system resides.
2. Issue authorization credentials for access.
3. Review the access list detailing authorized access by individuals annually and when personnel changes occur.
4. Remove individuals from the access list when access is no longer required.

B. Physical Access Controls. Enforce physical access authorizations by:

1. Verifying individual access authorizations before granting access.
2. Controlling ingress and egress using agency-implemented procedures and controls.
3. Maintain physical access audit logs for agency-defined sensitive areas.
4. Control access to areas designated as non-publicly accessible by implementing physical access devices including, but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers.
5. Escort visitors and control visitor activity in all physically secure locations.
6. Secure keys, combinations, and other physical access devices.
7. Inventory all agency-issued physical access devices annually.
8. Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

C. Transmission Access Control.

1. Control physical access to information system distribution and transmission lines and devices within facilities using agency-implemented procedures and controls.

D. Hardware Access Control.

1. Control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.

E. Physical Access Monitoring.

1. Monitor physical access to the DNR where the system resides to detect and respond to physical security incidents.
2. Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI or systems used to process, store, or transmit CJI.
3. Coordinate results of reviews and investigations with the division’s incident response capability.
4. Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

F. Visitor Recordkeeping

1. Maintain visitor access records for one year.
2. Review visitor access records quarterly.
3. Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.

4. Limit personally identifiable information (PII) contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected.

G. Emergency Procedures.

1. Provide an uninterrupted power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss. Protect power equipment and power cabling for the system from damage and destruction.
2. Provide the capability of shutting off power to all information systems in emergency situations.
3. Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel.
4. Protect emergency power shutoff capability from unauthorized activation.
5. Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
6. Employ and maintain fire suppression and detection systems that are supported by an independent energy source.
7. Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.
8. Maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels.
9. Monitor environmental control levels continuously.
10. Protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

H. Inventory Controls.

1. Authorize and control information system-related components entering and exiting the division.
2. Maintain records of the system components.

I. Alternate Work Sites.

1. Determine and document all alternate facilities or locations allowed for use by employees.
2. Employ security controls at alternate work sites:
    a. Limit access to the area during CJI processing times to only those personnel authorized to access or view CJI.
    b. Lock the area, room, or storage container when unattended.
    c. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
    d. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at-rest) of CJI.
3. Assess the effectiveness of controls at alternate work sites.
4. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

V. DIGITAL AND NON-DIGITAL MEDIA

A. Media Access and Storage.

1. Restrict access to digital and non-digital media to authorized individuals.
2. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.
3. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible.
4. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

B. Transporting Media.

1. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption, as defined in SC-13 and SC-28 of the CJI policy. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel.
2. Maintain accountability for system media during transport outside of the physically secure location or controlled areas.
3. Document activities associated with the transport of system media.
4. Restrict the activities associated with the transport of system media to authorized personnel.

C. Media use and disposal.

1. Restrict the use of digital and non-digital media on DNR owned systems that have been approved for use in the storage, processing, or transmission of CJI by using technical, physical, or administrative controls.
2. Prohibit the use of personally owned digital media devices on all DNR owned or controlled systems that store, process, or transmit CJI.
3. Prohibit the use of digital media devices on all DNR owned or controlled systems that store, process, or transmit CJI when such devices have no identifiable owner.
4. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration.
5. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

VI. ROLES AND RESPONSIBILITIES

A. Local Agency Security Officer: Ensure that policies and procedures required by the FBI CJIS Security Policy are developed and maintained. Ensure policies and procedures are disseminated and operationalized.
B. Division Information Technology staff: Develop, document, and disseminate to organizational personnel with physical and environmental protection responsibilities:

1. Agency-level physical and environmental protection policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    c. Includes Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls.

C. Designate personnel with information security responsibilities to manage the development, documentation, and dissemination of this policy and procedures.
D. Review and update the current physical and environmental protection:
    1. Policy annually and following any physical, environmental, or security related incidents involving CJI, or systems used to process, store, or transmit CJI; and
    2. Procedures annually and following any physical, environmental, or security related incidents involving CJI, or systems used to process, store, or transmit CJI.
    3. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.
    4. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.
    5. All division personnel will understand what constitutes physical, environmental, and media protection.

VII. COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

By Authority of:

_____

COL Rodmen Smith
Division Director
Division of Enforcement