DEPARTMENT OF CORRECTIONS

Policy Number:	**105.205**
Title:	**Computerized Information Resources Security**
Effective Date:	**1/27/25**

PURPOSE: To ensure the physical security of computerized information resources; ensure data integrity by protecting data from unauthorized access, modification, destruction, or disclosure; ensure compliance with the Minnesota Government Data Practices Act; and to recognize the valid rights of third parties in data and information resources utilized by the department. The department creates, uses, maintains, stores, preserves, and disposes of computerized information resources in accordance with requirements for government records and accepted data management practices.

APPLICABILITY: Department-wide

DEFINITIONS:

Backup – copy of a file, directory, or volume on a separate storage device from the original, for the purpose of recovery in case the original is erased, damaged, or destroyed.

Computerized information resources – data, the processes used to convert this into useful information, the equipment and technology required to use this information, and the people involved in making best use of the information.

Criminal Justice Data Communication Network (CJDN) – a computer network that is used to access state, federal, and out-of-state files for criminal justice use. Through the CJDN, the Minnesota Bureau of Criminal Apprehension (BCA) provides access to the Minnesota Justice Information Services (MNJIS) data, Driver and Vehicle Services (DVS) data, and Department of Natural Resources (DNR) data.

Encryption – any protective or disruptive measure, including but not limited to, cryptography, enciphering, or encoding that: (1) causes or makes any data, information, image, program, signal, or sound unintelligible or unusable; or (2) prevents, impedes, delays, or disrupts access to any data, information, image, program, signal, or sound.

Information technology (IT) security – develops, recommends, and monitors agency computer security guidelines.

Malware (short for "malicious software") – any intrusive software developed by cybercriminals (often called "hackers") to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.

Mobile computing device – includes a laptop personal computer, tablet personal computer, smartphone (including such examples as Android, Blackberry, Windows phone, and Apple iPhone), or any device that performs similar functions and may or may not connect to a department network.

Password – a form of confidential data authentication used to control unauthorized access to a resource.

Security incident – includes loss or theft of media (for example, paper, thumb drive, DVD) containing Criminal Justice Information (CJI), suspicious or malicious software in the local agency's environment, or unusual network activity.

Storage devices – items able to retain data, including such examples as CDs, DVDs, or portable flash and hard drives.

Strong password – combination of numbers, upper- and lower-case letters, and special characters/symbols.

Wireless local-area network (Wi-Fi) – a type of local-area network (LAN) that uses high-frequency radio waves rather than wires to communicate between nodes. Wi-Fi is a flexible data communication system used as an alternative to, or an extension of a LAN.

PROCEDURES:

A. <u>Data access and security</u>
    1. The department chief business technology officer (CBTO) maintains the integrity of computerized information resources and the authorization of access to those resources. The CBTO ensures security guidelines are developed in accordance with this policy to protect the integrity of department information resources. The CBTO/designee ensures users, contractors, and third parties having access to state computerized information resources are informed of and abide by this policy. The CBTO must:
        a) Ensure all security tools are current, operational, and do not disrupt the current technology environment;
        b) Ensure all access points are identified and controlled by an appropriate security method (physical, electronic, software, program control, etc.);
        c) Ensure user identifications (IDs) and passwords are implemented to allow access to computer resources via agency applications; and
        d) Ensure other, more secure methods are used for securing data if appropriate, including physical security (for example, locked room) or electronic security (for example, smart cards, biometrics and encryption).

    2. End users of computerized information resources are responsible for the security, integrity, and confidentiality of the data. Employees must:
        a) Ensure the information accessed is used responsibly to conduct department business;
        b) Provide passwords and change passwords on a regular basis using strong passwords;
        c) Ensure others do not have access to their individual passwords;
        d) Not share their individual IDs and passwords with others;
        e) Log off (secure) and/or lock (using ctrl/alt/delete function) computer workstations and be accountable for documents and communications created under their user ID. An automatic screen lock occurs if a workstation is left unattended. Workstations that perform a security related function (for example a workstation in a bubble or video display workstation) may be set to not lock automatically; these require the CBTO's approval; and
        f) Log their workstations onto the department network a minimum of once every thirty days.

    3. All individuals who have been approved to have access to department computer systems

are given appropriate role-based access (RBA) to the applications and systems necessary for them to perform their job responsibilities. User IDs and passwords regulate access to all systems. Sharing of user IDs and/or passwords is strictly forbidden. Unless a user ID is specifically designated for a defined group's use, user IDs and passwords are assigned to an individual. User ID and password use is restricted to that individual and must be kept confidential. Violators of user ID and password security may be subject to disciplinary action or criminal prosecution.

4. Database encryption and other advanced security controls are not allowed except when authorized by IT staff.

5. When a department employee separates employment or transfers within the department, the supervisor must ensure an off-boarding ticket request is created with all the necessary information.

6. Documents related to access control are retained securely by the IT unit.

B. Computer malware
1. IT unit staff members use malware detection and inoculation software to control malware.

2. IT unit staff members broadcast information, as necessary, to inform and provide procedures to employees of the presence and eradication of malware.

3. Employees must report any detected malware to the IT unit as soon as the malware is detected.

C. Disaster recovery/backup
1. The CBTO/designee ensures computer information resources are appropriately backed up and stored. Resources critical to the department must be stored in an off-site, secured storage facility available in the event of a disaster.

2. Each facility must develop and maintain disaster recovery security instructions or an emergency plan.

D. Authorized software
1. The IT unit must approve any software before installation on department equipment.

2. The IT unit provides employees the proper software license to purchase (new, product upgrade, competitive upgrade, etc.) based on the employee's current license.

3. The IT unit keeps reliable records of software use and purchases to ensure compliance with software licenses.

4. Any software added to department equipment must be added to the application inventory.

5. Employees must not make or use unauthorized copies of software.

6. IT units remove unauthorized copies of software, or the employee is required to purchase the appropriate licenses.

E.   Authorized hardware
      1.   The IT unit must approve any hardware that will be supported by the unit.

      2.   IT units maintain an inventory of computer equipment as a means of preventing and
            detecting theft of unsecured equipment.

      3.   The CBTO/designee must approve any non-department resource attaching to the
            department network. This includes contractor and consultant laptops.

F.   Auditing
      IT units must conduct unscheduled audits to verify software security tools, detect unauthorized or
      misuse of software or hardware, and to maintain the security and integrity of agency computer
      resources. The unit retains the audit results according to retention schedules.

G.   Wireless (Wi-Fi) networks
      1.   The CBTO/designee is solely responsible for the deployment and oversight of the
            management of department wireless networks and equipment. The IT unit ensures all
            wireless services deployed must adhere to department standards for access control.

      2.   The CBTO/designee must approve any handheld or personal wireless device before
            connection to department resources.

      3.   The IT unit, at its discretion and without prior notice, may disconnect any unauthorized
            wireless access points/base stations discovered on the department network, and may seek
            disciplinary action against the owner/operator of the device.

H.   CJDN terminals
      1.   The CJDN terminal computer must only be used for authorized access to criminal justice
            information such as computerized criminal history data, warrants, arrests, charges,
            convictions, probation, and placement in correctional facilities. It is also used to conduct
            background checks on individuals seeking employment or licensing for various positions.

      2.   The department maintains adequate physical security to all the CJDN terminals and
            stored/printed criminal justice data.

      3.   CJDN terminal areas must be restricted to the minimum number of employees necessary to
            perform the CJDN terminal function. Visitors to the terminal areas must be escorted at all
            times.

      4.   CJDN operators and those having unescorted access to the CJDN terminals must have a
            fingerprint-based background check prior to access.

      5.   Unauthorized access to CJDN terminals is not allowed.

      6.   If it has been determined that an individual has used a terminal for unauthorized purposes,
            disciplinary action may be taken.

      7.   All suspected security incidents must be reported to the BCA Information Security Officer
            within 24 hours of initial discovery at BCA.ISO@state.mn.us or (651)-793-2502 and
            through the attached link to the ISO Security Incident Response Report form.

8. Access to CJDN terminals is not permitted until training and certification is completed. All personnel with unescorted access to Criminal Justice Information must complete initial security awareness training and be re-certified annually.

I. Mobile computing and storage devices
1. Staff must immediately notify the department or correctional facility IT staff if a mobile computing or storage device is missing or compromised; if there is a loss of control of a device; or if a device loss or compromise takes place outside of the United States.

2. Non-departmental owned devices may connect (for example, through Wi-Fi) to the department guest network only.

3. Users of mobile computing and storage devices must diligently protect the devices from loss and disclosure of private or confidential information belonging to or maintained by the department.

4. IT staff provide mobile device management for state-owned devices. Exceptions may be granted by the commissioner of the DOC.

J. Employee new hire, transfer, or separation
At least five days prior to an employee new hire, transfer (which includes work out of class assignment), or separation, the employee's supervisor must complete a Minnesota Service HUB ticket. In addition, documents in accordance with Human Resources guidance (e.g. Onboarding Checklist) and any additional required documentation should be completed.

INTERNAL CONTROLS:
A. Software license, use, and purchase information is retained by the IT unit.

B. Information technology audits of software, hardware, security, resources, etc. are retained by the IT unit.

REFERENCES: Minn. Stat. §§13; 43A.38, subd. 4; 609.87 through 609.891
Policy 103.210, "Electronic Communications"
Policy 103.220, "Personal Code Conduct for Employees"
Policy 106.210, "Providing Access to and Protecting Government Data"
State of Minnesota MNIT Information Security Policies
MMB HR/LR Policy and Procedure #1423, "Appropriate Use of Electronic Communication and Technology"

REPLACES: Policy 105.205, "Computerized Information Resources Security," 6/19/18.
All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

ATTACHMENTS: Information Security Officer (ISO) Security Incident Response Report (BCA external link)

APPROVED BY:
Commissioner of Corrections