Minnesota Department of Corrections

Policy Number:	**105.205**
Title:	**Computerized Information Resources Security**
Effective Date:	**6/19/18**

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.

Computer virus – a computer program that can copy itself and infect a computer without permission or knowledge of the user. The original may modify the copies or the copies may modify themselves, as occurs in a metamorphic virus. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or carrying it on a removable medium such as a DVD, CD, or USB drive.

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 – the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information.

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

Mobile computing device – includes a laptop personal computer, tablet personal computer, smartphone (including such examples as 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.

Storage devices – include such examples as CD, DVD, or a USB flash drive.

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

Wi-Fi network – wireless local-area network (Wi-Fi) is a type of local-area network 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. Data access and security

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 (e.g. locked room) or electronic security (e.g. 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 ID 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 proper notification of information technology (IT) staff.

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

B. Computer virus

1. IT unit utilizes virus detection and inoculation software to control software viruses.

2. IT unit broadcasts information, as necessary, to inform and provide procedures to employees of the presence and eradication of malicious viruses.

3. Employees must report any detected viruses to the IT unit as soon as the virus 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. IT units must notify the central office IT unit of any new software installed on department equipment and regularly provide an inventory to the central office IT unit.

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. All personnel who have unescorted access the CJDN terminals must have a fingerprint based background check completed.

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

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.

2. Any non-departmental owned device that may connect (e.g., Wi-Fi) to the department network must first be approved by the CBTO/designee.

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. Prior to connecting a mobile computing and storage device, the user must ensure it is an approved device. The list of approved devices is available from department or correctional

facility IT staff.

5. Department IT staff provide mobile device security management to a select list of systems. The list of systems is maintained and made available by department IT staff.

6. All mobile devices must be encrypted by IT staff prior to leaving department grounds.

7. All laptops must be logged onto the department network a minimum of once every 30 days.

8. Department IT staff erase all mobile computing and storage devices prior to shipment for repairs or shipment to surplus services.

9. All mobile computing and storage devices must be encrypted.

J. Employee separation and transfer

1. Employee separation
At least five days prior to separation, the separating employee's supervisor must complete the IT Employee Separation Checklist (attached) and forward it to the department or facility IT staff. If it is an emergency and notification cannot be provided five days prior to separation, the employee's supervisor must immediately notify IT staff and provide the IT Employee Separation Checklist as soon as possible.

2. Employee transfer
At least five days prior to transfer, the employee's supervisor must complete the IT Employee Separation Checklist and forward it to the department or facility IT staff. The department or facility IT staff removes the employee's access on the last day of employment with the current unit. The employee's new supervisor must notify the department of facility IT staff of the employee's access requirements. The department or facility IT staff activates access to the employee's new requirements. If it is an emergency and notification cannot be provided five days prior to separation, the employee's supervisor must immediately notify IT staff and provide the IT Employee Separation Checklist, when applicable, as soon as possible.

3. Documentation
IT Employee Separation Checklists are retained by the staff person's facility IT unit, including the central office IT unit as appropriate, according to retention schedules.

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.

C. The IT units in central office and the facilities retain copies of completed Employee Separation Checklists.

ACA STANDARDS: 2-CO-1F-06

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," 4/16/13.
All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

ATTACHMENTS: IT – Employee Separation Checklist (105.205A)
Portable Electronic Storage Device Registration (105.205B)

APPROVED BY:
Deputy Commissioner, Facility Services
Deputy Commissioner, Community Services
Assistant Commissioner, Facility Services
Assistant Commissioner, Operations Support

Instructions
105.205CO, "DOC Central Office Visitor Wi-Fi Access"

Security Instructions (restricted access)
105.205-1CO (ALL FACILITIES), "Portable Electronic Storage Devices"