DEPARTMENT OF CORRECTIONS

Policy:	**303.040**
Title:	**Use of Electronic Equipment and Network by Incarcerated People/Residents**
Effective Date:	**11/4/25**

PURPOSE: To provide comprehensive controls and guidelines to ensure facility security and protect the public from the misuse of electronic equipment by incarcerated people/residents. This includes implementing robust cybersecurity measures to prevent unauthorized access to digital systems, protect sensitive information, and mitigate potential threats such as hacking, data breaches, or cyberattacks. By enforcing strict protocols on the use of electronic devices, this policy aims to safeguard facility operations, maintain the integrity of digital infrastructure, and prevent the exploitation of technology for illicit activities both within and beyond the facility. This policy governs the use, management, and security of electronic devices by incarcerated persons/residents to ensure compliance with state-wide cybersecurity standards and protect both facility operations and public safety.

APPLICABILITY: Minnesota Department of Corrections (DOC); all facilities under its jurisdiction. It also extends to the State of Minnesota's systems, infrastructure, and any electronic equipment or technology used within DOC facilities.

DEFINITIONS:

Administrative network – the internal computer network restricted for use by facility staff, providing access to administrative systems and resources.

Client network – the internal computer network designated for use by incarcerated persons/residents, facilitating controlled access to certain digital resources within the facility.

Electronic Device – any device that facilitates audio, video, text, or digital data transmission, including computers, smartphones, tablets, or other computer-like instruments.

Electronic equipment – any device or system capable of transferring, processing, or storing data, including such examples as computer hardware and software, telephones, digital cameras, storage media, and interactive televisions and whiteboards. This definition excludes personal property maintained by incarcerated individuals/residents in living units (for example, televisions, radios, vendor tablets, gaming systems), which is governed by a separate policy/directive. Further details regarding the use of electronic devices for post-secondary education are outlined in Policy 706.030, “Post-Secondary Education Student Use of Electronic Devices.”

Home folder – a designated electronic storage space allocated for incarcerated individuals/residents to store personal or educational files within the facility’s network.

Internet or online services – external computer networks that provide access to web-based or cloud-based resources beyond the facility's local systems.

Peripheral device – any external device connected to a computer via universal serial bus (USB), wireless connection, or other interfaces, such as printers, scanners, or external drives.

Restore software – software tools used by Minnesota Information Technology Services (MNIT) to restore workstations or devices to their authorized standard configuration or image.

PROCEDURES:

A. **Hardware/Software Forensic Inspections and Management**

1. Staff must notify Minnesota Information Technology Services (MNIT) staff or the MNIT helpdesk about any damage or malfunctioning electronic equipment.

2. All networked computers accessible to incarcerated people/residents must be automatically restored to a default state each night to ensure security and compliance.

3. A staff member at each facility is assigned to manage issues arising with incarcerated people's/residents' home drives. The education technology specialist monitors and controls the removal of folders.

B. **Equipment Safeguards**

1. Incarcerated people/residents may only use state electronic equipment for authorized education, library, reentry, treatment, or other specific work site purposes.

2. Incarcerated persons/residents are not allowed to tamper with electronic equipment. They may not use encryption, hidden files, or any other technology or techniques which could hinder or interfere with inspection.

3. Programming, code, job control language, or batch code must not be developed by an incarcerated person/resident without prior approval and under the direct supervision of a technically-qualified department staff person.

4. Peripheral devices must not be used in client networked computers without staff authorization.

5. Education, library, reentry, treatment, and other specific work site area staff/supervisors must monitor incarcerated persons'/residents' use of computers and are responsible to enforce computer use rules and expectations and to report policy violations.

6. Each work site area must post general computer use rules and expectations.

7. All voice and data communication lines located within a facility must be under the direct physical control of the facility staff.

8. Each incarcerated person is provided with a user account and home folder. The business unit designates staff to maintain user accounts (including password resets).

9. All contents of home folders are deleted from the client network 30 days after an incarcerated person's/resident's release.

C. **Authorized Use of Client Network**

1. Incarcerated people/residents may only use computers connected to the client network. Incarcerated people/residents are not allowed access to unnetworked computers without staff authorization. Incarcerated people/residents may not operate any designated staff equipment or administrative network equipment, including that which has access to any department management information systems.

2. Incarcerated people/residents are allowed to have access to the client network and have a home folder available for storing authorized documents.
   a) All documents created and saved on the client network are subject to inspection.

   b) The total amount of saved documents in a home folder must not exceed 20 megabytes of storage.

   c) Documents no longer relevant to current education or program status must be deleted by the incarcerated person/resident.

   d) Documents will automatically be deleted after one year of inactivity on those specific documents.

   e) Incarcerated people/residents must not share passwords or access to home drives.

   f) Documents created while incarcerated are not available after the incarcerated person/resident is released.

3. With prior staff permission, incarcerated people/residents may receive authorized printed material. Staff must review all printed material for approval before allowing an incarcerated person/resident to take possession of the materials. Each page printed by the incarcerated person/resident must have their name as a footer on the page.

4. Staff must monitor the incarcerated person's/resident's computer use.

5. Incarcerated people/residents must not store work items in individual home folders.
   a) Work areas must have work specific folders created for incarcerated/resident workers.

   b) Incarcerated workers'/resident workers' access to the work folders must be removed when the job assignment is ended.

6. Incarcerated people/residents must not attempt to visit unauthorized websites or download any unauthorized content, including such examples as photos, videos, or other images.

7. When leaving the computer station, the incarcerated person/resident must log out of their account.

D. **Authorized access to the Internet and staff-provided Internet materials**

1. Incarcerated people/residents are not permitted access to the Internet unless approved for work, educational, or programming purposes.

2. Case management, reentry, education, and other authorized program staff may provide Internet materials to incarcerated people/residents under the following circumstances:
   a) Incarcerated people/residents who are currently enrolled in an approved program or engaged in release planning for which the materials are directly related and appropriate to their program participation or release planning.

   b) Incarcerated people/residents who are requesting relevant legal research information through the facility law library or the Law Library Service to Prisoners (LLSP).

   c) Incarcerated people/residents who are requesting reference information (for example, zip codes, ISBN numbers, government and business addresses, and tax forms).

2. Incarcerated people/residents are not permitted access to the following Internet materials:
   a) Material prohibited by copyright law.

   b) Material excluded by DOC policy, including Policies 301.030, "Contraband;" 302.020, "Mail;" and 302.250, "Incarcerated Person Property."

E. Incarcerated people/residents may not possess electronic equipment outside the authorized area of use.

F. **Discipline and Violation Enforcement**

1. Unauthorized use of a computer will result in suspension from access to the client computer network and the removal of the documents.

2. In the case of unauthorized or contraband documents, all folders and documents will be removed from the incarcerated person's/resident's home folder.

3. Staff must report use violations by writing an incident report, and document them in the alleged violator's electronic file. Supervising staff must remove all contents of the incarcerated individual's/resident's home folder.

4. Incarcerated persons/residents may appeal the removal of documents by providing reasonable and specific justification on why specific documents should be returned. They will have 15 days to appeal documents they wish to have restored. Further appeals should be directed up the chain of command.

STATE CORRECTIONAL FACILITY SECURITY AUDIT STANDARDS: 3.03.03 through 3.03.08

INTERNAL CONTROLS:

A. Incarcerated person/resident violations, appeals, and appeal decisions are documented in their electronic files.

B. Business unit designees maintain lists of incarcerated person/resident passwords issued by supervisors.

REFERENCES:

Minn. Stat. § 243.556
Policy 204.045, "Library"
Policy 204.046, "Library – Juvenile Facilities"
Policy 300.300, "Incident Reports"
Policy 301.030, "Contraband"
Policy 302.020, "Mail"
Policy 302.250, "Incarcerated Person Property"
Policy 302.260, "Juvenile Resident Property"
Policy 303.010, "Incarcerated Individual Discipline"
Policy 303.015, "Informal Sanctions"
Policy 303.095, "Youth and Family Grievances"
Policy 303.100, "Grievance Procedure"
Policy 706.030, "Post-Secondary Education Student Use of Electronic Devices"

REPLACES:

Policy 303.040, "Use of Electronic Equipment and Network by Incarcerated People/Residents,"6/2/15.
All facility policies, memos or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

ATTACHMENTS: None

APPROVED BY:
Commissioner of Corrections