

CLIENT COMPUTER NETWORK

Minnesota Sex Offender Program

Issue Date: 9/1/20 Effective Date: 10/6/20 Policy Number: 120-5600

POLICY: Minnesota Sex Offender Program (MSOP) provides and maintains an internal computer and printer network for clients to use for legal work and other approved uses.

AUTHORITY: Minn. Stat. § 246.014, subd. (d)

APPLICABILITY: MSOP, program-wide

PURPOSE: To identify how, when, and for what purpose clients may utilize the internal client network and to maintain procedures for the administration and security of the network.

DEFINITIONS:

Business days – between 8:00 a.m. and 4:30 p.m. Monday through Friday, excluding legal holidays.

Client network – a designated network used by MSOP clients for approved use and for MSOP to communicate information. The client network cannot access the Internet, Education and Vocational Client Network (see MSOP Division Policy 120-5601, “Education and Vocational Client Network”), Department of Human Services’ (DHS) data systems, or external electronic systems.

Electronic equipment – computer hardware, software and printers.

Electronic information – data accessed through a computer.

Flash drive or other electronic storage device – a data storage device capable of interfacing with a computer.

Internet or on-line services – the World Wide Web, electronic chat rooms and peer-to-peer computer access.

Legal network space – a separate read-only network space where clients’ electronic files may be stored. These files are read-only electronic documents and data/documents from clients’ attorneys, other attorneys or from the courts. (See section E.3.a), below, for allowed file formats.)

MNIT – a division within the Minnesota Information and Technology Agency (MNIT) supporting the DHS.

MSOP Information Technology (IT) liaison – a staff designated at each facility to maintain server information and serve as a liaison for client and staff requests regarding the client network and MNIT staff.

Senior Management Team (SMT) – the Executive Director, the Deputy Director, and the Executive Clinical Director.

User Lock - works alongside Active Directory to protect access to Windows systems, with specific and customizable user login rules and real-time monitoring. User Lock reduces the risk of internal security breaches while helping to address regulatory compliance. This program permits clients to log-on to only those computers or their assigned living units.

PROCEDURES:

A. Usage

1. MSOP provides computer hardware, software and printers for clients to use for approved purposes in the library and on the residential living units. Clients are expected to use the computers in a respectful and responsible manner that is not wasteful or abusive.
2. Each client has 600 megabytes of network disk space in which to store electronic files.
3. Moose Lake site only
 - a) Each day clients in tier level 1 or 2 may sign up to use the unit computers, including those with legal research material, via sign-up sheets maintained by unit staff. Clients in tier level 3, 4, and 5 may use the unit computers, including those with legal research material, when available.
 - b) Each client in tier level 1 or 2 may initially reserve up to one hour of computer time.
 - c) After a client in tier level 1 or 2 has used his/her initial hour, the client may sign up for additional blocks of time in half-hour increments if a computer is available and no other client in tier level 1 or 2 is signed up to use the computers.
 - d) Once signed up to use the computer, a client may not transfer computer time to another client. Only the client who is signed up for the scheduled block of time may use the computer.
 - e) Clients in tier level 1 or 2 may use the regular library computers during their unit's scheduled times. Clients in tier level 3, 4 or 5 may use the library computers when available.
 - f) Clients whose restriction status prohibits them from using the unit computers are also restricted from using the library computers.
 - g) A client, even if restricted from general computer use, may sign up for an hour of time per day on their units' legal research computers, as space is available on a first-come, first-serve basis.
 - (1) To qualify for additional blocks of time on the unit legal research computer while on restriction, a client must have an upcoming court deadline falling within the period of time the client is on restriction.
 - (2) The client must submit a Client Request (420-5099a) to the client's unit group supervisor and show proof of the restriction and the court deadline.
4. St. Peter and Community Preparation Services (CPS) sites only
 - a) Clients in tier level 3, 4, or 5 or residing at CPS may utilize unit and library computers on a first-come, first-serve basis.
 - b) Clients in tier level 1 or 2 must coordinate access with unit team approval via an approved Client Request (420-5099a). Staff complete a Communication Log (410-5075a) (Phoenix) entry identifying the date and time the client is approved to use the computer.

- c) Clients needing the computer for treatment-related assignments take priority over clients using the computer for non-treatment-related reasons.

B. Maintenance

1. Designated MNIT staff at the specific facility reviews information on the client network quarterly.
2. MNIT works with the facility MSOP IT liaison to decide, in consultation with a member of the business area requesting posting of the information, if the information is out of date and should be removed.
3. The facility MSOP IT liaison works with the MSOP Records Manager to ensure compliance with data practices standards.

C. Inspections and Monitoring

1. Designated MNIT staff run reports monitoring client usage of the client computers for unauthorized activities or production of unauthorized files.
2. Designated MNIT staff provide reports for the Office of Special Investigations (OSI) and facility leadership review.
3. If a designated MNIT staff identifies potential unauthorized activities or unauthorized files on the client network (as outlined in section H below), the staff notifies his/her direct supervisor, who forwards the concern to MSOP SMT. To maintain the security of the network, designated MNIT staff may temporarily remove the computer from the network and inform the facility director.
4. If MSOP SMT has information that the network directory contains information or documents constituting a risk to the safety and security of the facility, specific individuals or the general public, or reasonable suspicion that a client is involved in criminal activities, then in consultation with the MSOP Legal and Records Director, they submit an email request to MNIT to search the client's network directory. The request to search must include a basis for the belief that the network directory contains information or documents constituting a risk to the safety and security of the facility, specific individuals or the general public, or reasonable suspicion that the client is involved in criminal activities.
5. If MSOP staff determine further investigation is warranted, they contact OSI to initiate investigation as outlined in DCT Policy 145-1010, "Investigations Involving Alleged Client Criminal Activity" and submit a work order through the MNIT Mall.
6. When a designated MNIT staff has reasonable suspicion a client has attempted to breach the client network or created or maintained data on the client network possibly compromising the safety and security of the network, designated MNIT staff may temporarily suspend the client's network access while seeking approval from the MSOP Executive Director, Deputy Director, or facility director to access and review those activities and files. The designated MNIT staff notifies the facility director and facility clinical director of the decision. The facility director notifies the client's program manager, CPS Operations Manager, and/or unit group supervisor.
7. If a client's access is temporarily suspended, the client's program manager, CPS Operations Manager, or unit group supervisor verbally informs the client that his/her access is temporarily

suspended, and completes a Communication Log (410-5075a) (Phoenix) entry regarding the reason for suspension.

8. Designated MNIT staff remove contraband items from the client network, after creating a backup copy of the contraband electronic files to be available for litigation and/or investigation purposes. The facility MSOP IT liaison sends the client a Contraband Notice (420-5250b) for such items.
9. Investigation Outcome:
 - a) If the review of the client's network space determines no misuse occurred, MNIT staff immediately restore the client's access.
 - b) If the review of the client's network space determines misuse occurred, MNIT and/or OSI refer the matter to the Behavioral Expectations process (see MSOP Division Policy 420-5010, "Client Behavioral Expectations").
 - c) If the review of the client's network space takes longer than ten business days, OSI reviews the client's continued suspension in consultation with the facility director and facility clinical director to determine when access is re-instated. The client's program manager, CPS Operations Manager, or unit group supervisor documents the decision in an Individual Progress Note (215-5007d-4020) (Phoenix).
10. MSOP utilizes the User Lock program for all clients residing on unit Omega. Unit security staff submit a work order through the MNIT Mall when clients are moved on, off, or within the Omega units to ensure the User Lock feature is applied appropriately. The assistant facility director/designee may identify other clients who are subject to the User Lock program based on safety and security and provide their names to the facility MSOP IT liaison.

D. Printing - Clients use their own paper to print documents on the MSOP-provided network printers. Clients may not print material prohibited under MSOP Division Policy 420-5230, "Media Possession by Clients" or considered contraband under MSOP Division Policy 415-5030, "Contraband," or MSOP Division Policy 225-5310, "CPS Contraband." Staff scan the printed material prior to giving it to the client to ensure it does not contain contraband.

E. Incoming Legal Materials

1. Clients may not receive incoming flash drives or other electronic storage devices. (See MSOP Division Policy 415-5030, "Contraband," or MSOP Division Policy 225-5310, "CPS Contraband.")
2. If a client receives a flash drive or other electronic storage device from a verified attorney or from a court, the facility Special Services or unit staff who opened the legal mail asks the client if he/she would like to have the electronic information added to the client's legal network space.
 - a) The facility Special Services or unit staff inventories the flash drive or other electronic storage device on a Notice and Receipt of Secured Items (420-5250a), indicating whether or not the client chooses to have the electronic information added to the client's legal network space.
 - b) If the client chooses to have the electronic information added to his/her legal network space, the facility Special Services or unit staff forwards the electronic storage device

and the Notice and Receipt of Secured Items (420-5250a) directly to MNIT staff to be copied onto the client's legal network space.

- c) If a client chooses not to have his/her legal electronic information placed on the client's legal network space, the facility Special Services or unit staff forwards the electronic storage device and the Notice and Receipt of Secured Items (420-5250a) to the facility Special Services Department for processing as contraband.
3. Designated MNIT staff copy the material from the flash drive or other electronic storage device into the client's legal network space, when the client chooses to have the information added.
- a) Before copying the electronic information into the client's legal network space, the designated MNIT staff visually scans the material for contraband.
 - (1) Password-protected files preventing MNIT staff from visually inspecting the material on the electronic storage device(s) are contraband and will not be uploaded to a client's network space.
 - (2) Documents must be compatible with Microsoft Word or Adobe Reader. Audio files must be compatible with Windows Media Player. Worksheet files must be compatible with Microsoft Excel. Image files must be compatible with either Windows picture or Microsoft Paint applications. All other programs and files are contraband.
 - b) Designated MNIT staff transfer the material to the client's legal network space within two business days upon receipt by MNIT.
 - c) Designated MNIT staff place files in electronic folders on the legal network space and label the folders to reflect the dates the files were received.
 - d) Upon transferring material to the client's legal network space, designated MNIT staff forward the flash drive or other electronic storage device to the facility Special Services Department for processing as contraband.
4. A client may review and print material from his/her legal network space, but may not modify the material in this space.

F. Outgoing Legal Material

Clients wishing to send electronic material out of the facility may print and mail out the documents. If a client is legally scheduled to depart the MSOP, as defined per MSOP Division Policy 230-5100, "MSOP Departure," the client may request the facility MSOP IT liaison to copy the client's electronic files from the client network space and send the files to a designated address.

G. Client Network ID Assignment/Maintenance/Password Security

1. Designated MNIT staff assign computer login passwords to clients.
2. The facility MSOP IT liaison notifies designated MNIT staff when a client transfers between MSOP sites, to have client data on the client network transferred with the client.

H. What Clients May and May Not Do on the Client Network

1. Clients may use the client network for:
 - a) treatment assignments;

- b) personal Word or Excel processing;
 - c) reviewing data requests per MSOP Division Policy 135-5170, "Data Request and Copy Costs";
 - d) legal research and work; and
 - e) other uses as approved by a client's primary therapist via a Client Request (420-5099a).
2. The following activities are prohibited on electronic equipment:
- a) sharing a username and/or password with other individuals;
 - b) tampering with or removing security devices;
 - c) altering a computer configuration, either physically or programmatically;
 - d) creating or storing unauthorized files;
 - e) creating or storing password-protected files
 - f) conducting intentional activities to damage the computers or other electronic equipment and/or peripherals (e.g., keyboard, mouse, etc.);
 - g) creating, sharing, or storing contraband;
 - h) modifying the network environment;
 - i) accessing removable and/or external files and media; or
 - j) sharing username and password for the sole reason to communicate on the network covertly with other MSOP clients.
3. The client computers do not retain preferences.

I. Requests

Clients may submit a Client Request (420-5099a) to the facility MSOP IT liaison, and the liaison submits it to MNIT staff for the following requests (except as otherwise noted below).

1. Clients may change their computer passwords by submitting a Transfer Authorization (125-5300d) to Direct Care and Treatment (DCT) Financial Services. Once processed, DCT Financial Services staff change the client's personal identification number (PIN) in Global Tel Link (GTL) and submit a work order for the PIN to be updated.
 - a) To unlock an account, a client must provide his/her login information, starting with the letter "c."
 - b) An account locked out due to an invalid password resets after approximately sixty minutes.
2. To request the restoration of deleted files, a client must provide his/her network login identification along with the name of the deleted files when submitting a Client Request (420-5099a) to the facility MSOP IT liaison within two days after finding the file is missing. To facilitate retrieval efforts, the client should indicate the approximate date(s) of last use or deletion (if known) on the Client Request (420-5099a). Depending on the length of time between the deletion of a file and notification of MNIT, IT staff might be able to restore the file. MNIT may take up to five business days from receipt of the request to restore the files.
3. If a client notices any hardware or software issues with the computers, the client submits a Client Request (420-5099a) to the facility MSOP IT liaison and the liaison works with designated MNIT staff to assess and fix the problem within five business days from receipt of the request.

J. Staff Use of Client Network for Posting Purposes

1. Upon staff request, the facility MSOP IT liaison/designee at each facility may forward the following posting requests to designated MNIT staff to place them on the client network without consulting the facility director and facility clinical director/designee:
 - a) client menus;
 - b) MSOP policies and approved media lists;
 - c) client memos;
 - d) minutes from the client representative meetings;
 - e) vocational opportunity postings;
 - f) tax forms (around tax season);
 - g) absentee ballots applications;
 - h) DHS applications for General or Medical Assistance;
 - i) household report form;
 - j) Minnesota application for a birth certificate;
 - k) application for a replacement Social Security card;
 - l) voter registration application;
 - m) data requests;
 - n) approved spiritual items (e.g., schedules or calendars of upcoming spiritual events); and
 - o) supplemental learning tools.

2. For any posting requests not listed in J.1 above:
 - a) the facility MSOP IT liaison or the MSOP Policy and Compliance Director must obtain the approval of the facility director and the facility clinical director/designee prior to sending the item(s) to MNIT for upload; and

 - b) as needed, the facility MSOP IT liaison posts an announcement on the unit bulletin boards informing clients what and where the item is posted.

3. MNIT staff post on the client network only information sent by the facility MSOP IT liaison, MSOP Policy and Compliance Director, or MSOP Legal and Records Director.

K. Service Interruptions

1. MSOP may temporarily disable all or part of the client network to maintain security, perform maintenance, or respond to any compromise of the network.

2. If a client locks up a computer by mistyping his/her password or username, the system resets in approximately 60 minutes and the client may sign in again.

3. In the event of a long-term service outage, MNIT staff make a reasonable effort to provide clients with computer access. A long-term outage could last up to five business days. The facility MSOP IT liaison or unit staff informs clients about the status of the outage.

4. MNIT support personnel are available during business days to resolve client network issues and to restore services. Issues arising outside normal business hours must wait until the next business day.

REVIEW: Annually

REFERENCES: MSOP Division Policy 135-5100, "Confidentiality and Data Privacy"
MSOP Division Policy 420-5230, "Media Possession by Clients"
MSOP Division Policy 415-5030, "Contraband"

MSOP Division Policy 225-5310, "CPS Contraband"
MSOP Division Policy 420-5010, "Client Behavioral Expectations"
MSOP Division Policy 230-5100, "MSOP Departure"
MSOP Division Policy 410-5200, "On-Call"
MSOP Division Policy 135-5170, "Data Request and Copy Costs"
MSOP Division Policy 410-5075, "Communication Log"
DCT Policy 145-1010, "Investigations Involving Alleged Client Criminal Activity"
DCT Division Policy 215-5014, "Client Tier Level System"
Minnesota Statutes, Chapter 13
Health Insurance Portability and Accountability Act (HIPAA)

ATTACHMENTS: Transfer Authorization (120-5300d)
Client Request (420-5099a)
Contraband Notice (420-5250b)
Notice and Receipt of Secured Items (420-5250a)
Individual Progress Note (215-5007d-4020) (Phoenix)
Communication Log (410-5075a) (Phoenix)

SUPERSESSSION: MSOP Division Policy 120-5600, "Client Computer Network," 2/5/19.
All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

/s/
Nancy A. Johnston, Executive Director
Minnesota Sex Offender Program