CLIENT COMPUTER NETWORK
Minnesota Sex Offender Program

Issue Date: 11/7/23 Effective Date: 12/5/23 Policy Number: 120-5600

.

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

Electronic storage device – a data storage device capable of interfacing with a computer.

Internet – 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 – Minnesota Information and Technology Services (MNIT) supporting the DHS.

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

Treatment team – see MSOP Division Policy 215-5005, "Treatment Overview."

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 designated client computers.

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. MSOP utilizes User Lock for clients residing on Units Omega 1 and 2 and the High Security Area (HSA).
   a) Unit staff submit a work order through the Minnesota Service Hub when clients are moved on, off, or within Omega 1/2 or the HSA to ensure the User Lock feature is applied appropriately.

   b) The assistant facility director/designee may identify other clients who are subject to the User Lock program based on safety and security and provide client names to the facility MSOP IT liaison.

4. Moose Lake site only
   a) Clients in tier level 3, 4, and 5 may use the unit computers, including those with legal research material, when available.

   b) Clients in tier level 1 or 2 may sign up each day to use the unit computers, including those with legal research material, via sign-up sheets maintained by unit staff.
      (1) A client may initially reserve up to one hour of computer time.

      (2) After the client has used the 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.

      (3) 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.

   c) Clients in tier level 3, 4, or 5 may use the library computes when available. Clients in tier level 1 or 2 may use the library computers during their unit's scheduled times.

   d) Clients whose restriction status prohibits them from using the unit computers are also restricted from using the library computers.

   e) A client, even if restricted from general computer use, may sign up for an hour of time per day on a unit's legal computers, as space is available on a first-come, first-serve basis.
      (1) To qualify for additional blocks of time on the unit legal 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.

5. 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 computer access with unit treatment 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. Client Network ID Assignment/Maintenance/Password Security
1. MNIT staff provide computer login passwords to clients.

2. The facility MNIT liaison or unit staff submits a work order through the Minnesota Service Hub when a client transfers between MSOP sites to have client data on the client network transferred with the client.

C. 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:
   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.

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 electronic storage devices. (See MSOP Division Policy 415-5030, "Contraband," or MSOP Division Policy 225-5310, "CPS Contraband.")

2. If a client receives an 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 the client 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 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 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) directly to MNIT staff via work order through the Minnesota Service Hub to copy the information onto the client's legal network space.

   c) If a client chooses not to have the client's 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. MNIT staff copy the material from the 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 MNIT staff visually scans the material for contraband (refer to MSOP Division Policy 415-5030, "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) MNIT staff transfer the material to the client's legal network space within two business days upon receipt by MNIT.

   c) 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, MNIT staff forward the electronic storage device to the facility Special Services Department for processing as contraband.

4. A client may review and print material from the client's 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 MSOP as defined per MSOP Division Policy 230-5100, "MSOP Departure."

1. The client may submit a Client Request (420-5099a) to the facility MSOP liaison requesting a copy of the electronic files from the client's network space and detailing the designated address for the files to be sent.
2. The facility MSOP IT liaison submits a work order through the Minnesota Service Hub for the MNIT staff to make a copy of the requested files.
3. The MNIT staff provides the copies of the files to the MSOP IT liaison to be sent to the designated address.

G. 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 ViaPath and submit a work order for the PIN to be updated.
   a) To unlock an account, a client must provide the 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 the 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 may or may not be able to restore the file. MNIT may take up to five business days from receipt of the request to attempt 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/designee and the liaison works with MNIT staff to assess and attempt to fix the problem within five business days from receipt of the request.

H. Staff Use of Client Network for Posting Purposes

1. Staff may submit a work order through the Minnesota Service Hub attaching the following posting requests to MNIT staff for placement 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);
o) supplemental learning tools; and
p) Quarterly MSOP Community Newsletter (see MSOP Division Policy 220-5200, "Community Newsletter").

2. For any posting requests not listed in H.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.

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

3. Posting Retention
   a) MNIT staff review information on the client network each quarter.

   b) MNIT staff work with the facility MSOP IT liaison to decide, in consultation with a member of the business area posting the information, if the information is out of date and should be removed.

   c) The facility MNIT liaison works with the MSOP Records Manager to ensure compliance with data practices standards.

I. 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 the 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.

J. Client Network Monitoring
1. Usage Reports

a) MNIT staff run reports monitoring client usage of the client computers for unauthorized activities or production of unauthorized files.

b) Office of Special Investigations (OSI) staff request reports from MNIT staff to review.
   (1) OSI notifies the facility director/designee if any information appears suspicious.

   (2) If appropriate, staff may initiate a Request for Client Network Search (120-5600a) may be initiated as outlined in section K below.

2. Client Network Misuse
   a) Unauthorized Activity/Files
      (1) MNIT staff complete an Incident Report (410-5300a) (Phoenix) when discovering unauthorized activity or unauthorized files on the client network (see MSOP Division Policy 410-5300, "Incident Reports").

      (2) MNIT staff may remove unauthorized files from the client network after saving a digital copy for investigation and/or litigation purposes. MNIT staff place the digital copy on a disc and secure the disc as evidence (see DCT Security Policy 145-1035, "Evidence Handling by Staff"). The facility director/designee ensures the Notice and Receipt of Secured Items (420-5250a) is completed in accordance with MSOP Division Policy 420-5250, "Client Property" or MSOP Division Policy 225-5300, "CPS Client Property."

      (3) The facility director/designee may:
         (a) refer the matter to the behavioral expectations process (see MSOP Division Policy 420-5010, "Client Behavioral Expectations" or MSOP Division Policy 225, 5025, "Client Accountability System"); and/or

         (b) contact OSI to initiate an investigation as outlined in DCT Policy 145-1010, "Investigations Involving Alleged Criminal Activity."

   b) Client Network Suspension
      (1) If MNIT staff have reasonable suspicion a client has attempted to breach the client network or created/maintained data on the client network possibly compromising the safety and security of the network or facility, MNIT staff may temporarily suspend the client's network access while seeking approval from the MSOP Executive Director or facility director to access and review those activities and files. MNIT staff notify the facility director and facility clinical director of the decision. The facility director notifies the client's treatment team.

      (2) Desingated MNIT staff complete an Incident Report (410-5300a) (Phoenix) when detailing the reasons for the client network suspension (see MSOP Division Policy 410-5300, "Incident Reports").

      (3) If a client's access is temporarily suspended, the assistant facility director/designee verbally informs the client that access is temporarily suspended, completes a Communication Log (410-5075a) (Phoenix) entry regarding the suspension, and notifies the client's clinical supervisor and/or unit director.

(4) If suspension lasts longer than ten business days due to ongoing review, the facility director reviews the client's continued suspension in consultation with the facility clinical director to determine if continued suspension is necessary. If continued suspension is necessary, the assistant facility director/designee documents the decision via the Communication Log (410-5075a) (Phoenix).

(5) The assistant facility director/designee informs the client when the client's access to the client network is restored and completes a Communication Log (410-5075a) (Phoenix) entry.

(6) The facility director/designee may:

(a) refer the matter to the behavioral expectations process (see MSOP Division Policy 420-5010, "Client Behavioral Expectations" or MSOP Division Policy 225, 5025, "Client Accountability System"); and/or

(b) contact OSI to initiate an investigation as outlined in DCT Policy 145-1010, "Investigations Involving Alleged Criminal Activity."

K. Client Network Search

1. Staff may initiate a Request for Client Network Search (120-5600a) for a specific client network space when based on articulated objective information.

a) The assistant facility director/designee or OSI must submit a completed Request for Client Network Search (120-5600a) for review prior to the search. The request must include the following criteria:

(1) there is reasonable suspicion the client network contains information or documents constitution a risk to facility safety and security, specific individuals, or the public; and or

(2) there exists reasonable suspicion a client is involved in criminal activity on the client network.

b) If approved by the facility director and MSOP Legal and Records Director, the requestor contacts MNIT staff to initiate the client network search.

c) MNIT staff conduct the search and provide the search results to the requestor for review.

2. Client Network Search Outcome

a) The assistant facility director/designee:

(1) if the review of the client's network space determines misuse occurred, documents the computer misuse via an complete an Incident Report (410-5300a) (Phoenix) and refers the matter to the behavioral expectations process (see MSOP Division Policy 420-5010, "Client Behavioral Expectations" or MSOP Division Policy 225, 5025, "Client Accountability System"); and/or

(2) contacts OSI to initiate an investigation as outlined in DCT Policy 145-1010, "Investigations Involving Alleged Criminal Activity."

b) OSI staff:

(1) document the computer misuse via an Incident Report (410-5300a) (Phoenix); and/or

(2) follows DCT Policy 145-1010, "Investigations Involving Alleged Criminal Activity" if the review of the client's network space indicates alleged criminal activity.

REVIEW: Biennially

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 Criminal Activity"
DCT Division Policy 215-5014, "Client Tier Level System"
MSOP Division Policy 215-5005, "Treatment Overview"
MSOP Division Policy 220-5200, "Community Newsletter"
MSOP Division Policy 410-5300, "Incident Reports"
DCT Security Policy 145-1035, "Evidence Handling by Staff"
MSOP Division Policy 420-5250, "Client Property"
MSOP Division Policy 225-5300, "CPS Client Property"
MSOP Division Policy 225, 5025, "Client Accountability System"
Minnesota Statutes, Chapter 13
Health Insurance Portability and Accountability Act (HIPAA)

ATTACHMENTS:
Request for Client Network Search (120-5600a)

Transfer Authorization (120-5300d)
Client Request (420-5099a)
Contraband Notice (420-5250b)
Notice and Receipt of Secured Items (420-5250a)
Communication Log (410-5075a) (Phoenix)
Minnesota Service Hub-MSOP VocEd/Client Network Reporting Request
Incident Report (410-5300a) (Phoenix)

SUPERSESSION: MSOP Division Policy 120-5600, "Client Computer Network," 10/5/21.
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