dmhas
A Healthcare
Service Agency

**STATE OF CONNECTICUT**
**Department of Mental Health & Addiction Services**

## Commissioner's Policy Statement and Implementing Procedures

| | |
|---|---|
| **SUBJECT:** | Computer Access Controls |
| **P & P NUMBER:** | Chapter 7.4 |
| **APPROVED:** | Miriam Delphin-Rittmon, Commissioner Date: 10/15/2015 |
| **EFFECTIVE DATE:** | October 15, 2015 Miriam Delphin-Rittmon |
| **REVISED:** | 11/1/2012 |
| **REFERENCES:** | The following are links to the Department of Administrative Services/Bureau of Enterprise Services and Technology (DAS/BEST) Policies, which the Department of Mental Health and Addiction Services (DMHAS) abides by:<br>● **Acceptable Use of State Systems (Internet and E-Mail)**<br>● **Telecommunications Equipment**<br>● **Network Security and Procedures**<br>● **State Property Control**<br>● **Security for Mobile Computing and Storage Devices**<br>● **HIPAA Security Policy**<br>● **Social Media Policy**<br>● **Implementation/Deployment of State Agency Internet Sites and Extranet Sites** |
| **FORMS AND ATTACHMENTS:** | |

**STATEMENT OF PURPOSE:** The Department of Mental Health and Addiction Services (DMHAS) abides by the policies set forth by the Department of Administrative Services/Bureau of Enterprise Services and Technology (DAS/BEST) relating to access to systems. The State of Connecticut (SOC) has developed a comprehensive set of acceptable use policies for networking, telecommunications and electronic mail systems.

**POLICY:** The Information Technology (IT) Department shall work with the local IT support to procure and maintain all Network access, security, logins, hardware and support for all the Department of Mental Health and Addiction Services (DMHAS) Staff. It is the user's responsibility to keep his/her data secure by: logging out of the Network when not in use, never sharing or giving one's password to anyone, never writing down one's password where it is easily accessible, not storing data locally and by reporting to the Information Technology (IT) Department any breach or potential breach of security.

1. Users will be prompted to change their passwords every sixty days.
2. Users will keep their data on the Network drives and no data will be kept on the local computers.

3. All traffic on the Network, including e-mail and the Internet, may be monitored by the Bureau of Enterprise Services and Technology (BEST), and the Department of Mental Health and Addiction Services (DMHAS).

4. Patients are not allowed to use staff computers or access the Department of Mental Health and Addiction Services (DMHAS) Network.

5. No personally owned items can be used on our computers as stated in the Commissioner's Policy Statement No. 82. This includes keyboards, mice, laptops, printers, external drives, modems, thumb drives, USB devices or anything else.

6. The Department of Mental Health and Addiction Services (DMHAS) does not allow the use of floppy diskettes, memory sticks, zip drives, mini hard drives or Personal Data Assistants (PDA) unless there is written permission from the Information Technology (IT) Manager.

## PROCEDURE:

A. The Network has various drives which allow users to share data in a secure environment, store data in a unique place for each individual and access data which has been purchased for any employee at the Hospital.

To obtain access to the Department of Mental Health and Addiction Services (DMHAS) Network, the user will also be given the State of Connecticut (SOC) Acceptable Use of state systems policy and will need to sign the Acknowledgment of receipt of State Acceptance. They will also be given an Access Request Form to fill out and submit to the Information Technology (IT) Department. The form should be signed by the employee and the Division/Department Director or his/her designee. After the Information Technology (IT) Department has created the LAN/email account, they will contact the user or person designated in the department who is responsible for notifying the user.

For Security purposes, when a user calls the Local IT staff or the central Information Technology (IT) Department to have their password reset, they will need to provide their employee identification number.

Staff having any problems with the Network should contact their local IT support and in if the local IT support needs assistance they will contact central Information Technology (IT) help desk at 860-262-5058. If it is an emergency or off normal business hours and there are no off hours support locally then the user they should contact their local Information Technology (IT) support if applicable or they should call 860-262-5000 (IT) help desk and have the on call technical support person paged.

1. *"User" Drive:* The User (U) drive is a place for users to store documents and data only. It is not for any other file types. The Information Technology (IT) Department will periodically search the User (U) drives for files which are not allowed, including: program, link, music, and executable files. Files with the following extensions will be removed: (EXE, COM, MP3, MP, DAT, TMP, INI, WPG, JPG, BMP, DLL, and LNK). The User (U) drive is backed up daily and is a secure folder for each individual. It is the user's responsibility to backup their data. The following folders will be deleted from the User (U) drives: Application Data that contains the folders (Adobe, Identities, Inter trust, Microsoft), Cookies, Desktop, History, Muzik, Games, Real Jukebox and Real Player. If a user transfers to another location, any data stored on his/her User (U) drive pertaining to their old assignments should be reviewed with their Supervisor and removed, if needed.

2. *"T" drive*: The "T" drive or Groups on the "T" drive is a place for two or more users to share data in a secure environment.

   Groups on T: or the "T" drive: The "T" drive is unique to each user. In order to have a folder created on the "T" drive, a user should submit a Group Access Request form to the Information Technology (IT) Department, specify what a user would like the folder to be called, who a user would like to have access to the folder and what rights a user would like the other users to have. There are two options for "Rights": Read Only, or ALL, which includes the ability to erase files. The user requesting the folder be created then becomes the "Owner" of the folder. The Information Technology (IT) Department will send an email to the requestor confirming the folder has been created. The requestor will then notify the other users. The Information Technology (IT) Department can help answer any questions regarding new folders or existing folders on the "T" drive. If a user Transfers to another location, it is his/her responsibility to notify the Information Technology (IT) Department and his/her former supervisor of the folders they have access to on the "T" drive.

   Users requesting access to existing folders on the "T" drive, need to submit a LAN Access Request form to the Information Technology (IT) Department. The Information Technology (IT) Department will send an email of the LAN Access Request form to the "Owner" of the folder for approval. Upon approval, the user will be added to the folder and the Information Technology (IT) Department will send a confirmation notification. If the user's request was rejected by the Owner, the Information Technology (IT) Department will send a notification to the requestor.

3. ***"S"** Drive:* The "S" drive is for users to post notices of interest for all employees to view. Users cannot write to the "S" drive, but can request items be posted through the Information Technology (IT) Department.

Users requesting an item to be posted on the “S” drive, needs to send an e-mail attachment to the Information Technology (IT) Department or designee with the item they want posted. If the Information Technology (IT) Department Manager feels there is an issue with the item, they will call or email the user to arrange a time to discuss the concerns.

B. *Passwords:* User passwords will expire every sixty days. The user will need to enter a unique password when his or her account has expired.

Rules on passwords:

a. Minimum of six letters or more.
b. Can be combination of letters and numbers.
c. Cannot use “Special” characters (?;>;<;!;@;#;$;%;^;&;(); etc. ).
d. Cannot start with a 0 (zero).
e. Do not use identifiable information (login name, SSN, DOB, children’s or spouse’s names, titles, and pet’s names).
f. Try to make your password difficult for someone to guess.

C. *Viruses:* The Information Technology (IT) Department will make sure that each computer has up to date virus protection software.

D. *Employment change (Terminations/Transfers/Retirements):* The Human Resources (HR) Department notifies the Information Technology (IT) Department of all hires, terminations, retirements and transfers for the facilities. Upon receiving this list, the Information Technology (IT) Department disables these employees from all systems on the date of termination provided by the Human Resources (HR) Department. After the employee is disabled from all systems, his/her User (U) drive and e-mails are no longer accessible. It is the departed workers Supervisor who is responsible to ensure that the employee who is leaving has transferred any files needed to the designated person prior to their last day.