NORTH COUNTRY COMMUNITY MENTAL HEALTH

ADMINISTRATIVE MANUAL

CHAPTER: Nine – Management of Information
SECTION: Two – Information Systems
PROTOCOL NAME: INFORMATION SYSTEMS ACCEPTABLE USE PROTOCOL
EFFECTIVE DATE: August 1, 2013

PURPOSE

To educate and validate that all NCCMH staff understand acceptable uses for NCCMH Information Systems.

APPLICATION

All North Country Community Mental Health Programs.

PROTOCOL

Only staff will use the computer User Account(s) provided to them and they will take the responsibility to protect their account(s) from unauthorized access. Staff will not allow anyone else to use their User Account.

1. Passwords

Staff will be issued a user ID and a password to authenticate their computer account. They understand that they will be requested to change their password at specified intervals, although they may elect to do so at more frequent intervals if they believe that the privacy of their password has been compromised. This rule is primarily intended for the protection of their User Account(s) and its data.
After receiving their password—

- Staff will not allow anyone else to have or use their password. If staff knows that their password is compromised, they will report to their System Administrator (SA) for a new one.
- Staff understands the use of strong passwords is recommended.
    - To create a strong password use a combination or all of the following
        - No less than 8 characters long
        - Alpha and numeric values
        - Upper and lowercase letters
        - Symbols such as &, $, @

- If staff write down their password it will be kept in a locked location
- Staff is responsible for all activity that occurs on their individual account once their password has been used to log on.
- Staff will not store their password on any processor, microcomputer, personal digital assistant (PDA), or on any magnetic or electronic media.

2. Access

Facilities are available for the conduct of agency business, i.e., research, instruction, health care and administration. No other uses are permitted.

- Staff will use agency information systems (computers, systems, and networks) only for authorized purposes.
- Staff shall not use the agency's computing facilities for any form of private financial gain.
- Staff understands that access to the agency's computing facilities by unauthorized persons or for unauthorized purposes is forbidden. Staff shall not use agency computing facilities in any way that intentionally compromises their availability or effectiveness to other individuals. Some examples are presented for clarification:

- Attempts to access restricted portions of an operating system, accounting software or the private file space of other users;
- Use of information systems in such a way as to disrupt the operation of computer or communication systems within or outside of the agency;
- Attempts to breach security mechanisms or exploit or publicize problems that might exist in them;

- Staff shall not use their computer account privileges to attempt access to computing facilities within or external to the agency to which they have not received prior authorization.
- Staff will not try to access data or use operating systems or programs, except as specifically authorized.

If staff has information regarding attempts to breach the security of the agency's computer facilities, they agree to promptly report such information to the Information Systems Director.

3. Software/Copyright

- Staff agrees to abide by any patent or copyright restrictions which may relate to the use of computing facilities, products, programs or documentation.
- Staff agrees not to copy, disclose, modify or transfer any such materials that they did not create, without the expressed consent of the original owner or copyright holder.
- Staff agrees not to use the agency's computing facilities in any way which violates the terms of any software license agreement, or any applicable local, state or federal laws.
- Staff will not import or load any software or install hardware on any agency computer (for example, client-workstation or server) without first getting prior approval from their supervisor.
- Staff will not download file-sharing software (including MP3 music and video files), peer-to-peer software (i.e. Kazaa, Napster) or games onto their agency computer, system, or network.
- Staff will not copy any agency data or PHI on to any removable media such as CDs, DVDs, flash, thumb, or external drives without prior authorization from their supervisor.
- Staff will recognize that data and software on agency computers, systems, and networks is the property of the agency and may not be copied to any personal device for use outside of work.

4. Security

- If staff observes anything on the system they are using that indicates inadequate security, they will immediately notify the IS Department.
- Staff will never leave their agency computer unattended while they are logged on unless the computer is protected by a "password protected" screensaver.
- Staff will not connect NCCMH removable media to non agency computers except for the purpose of presentations or printing off site. In these circumstances, the removable media cannot contain any PHI.
- Staff will not connect any personal IT equipment (for example, PDAs, personal computers, cameras, flash media, and digitally enabled devices) to their agency computer or to any agency network without the approval of the Information Systems Director.
- Staff will not use Internet "chat" services [for example, America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo] from their agency computer.
- Staff will not forward chain e-mails. Emails warning of a virus are not to be forwarded either.

Staff understand that non-compliance with this Agreement may result in denial or removal of access privileges to the agency's electronic systems; disciplinary action as set forth by other agency policies and guidelines, civil litigation; and/or criminal prosecution under applicable state and federal statues.

Staff knows that their actions as a user can greatly affect the security of the system and that their signature on this agreement indicates that they understand their responsibility as a user requires that they adhere to regulatory guidance.

REFERENCE:

REVISED: July 15, 2013

APPROVED BY SIGNATURE:

Alexis Kaczynski	*7/15/2013*
Director	Date
Dianne Forster	*7/22/2013*
MIS Director	Date