NORTHERN NEVADA ADULT MENTAL HEALTH SERVICES (NNAMHS)

POLICY AND PROCEDURE

SUBJECT: COMPUTER USE POLICY

NUMBER: NN-HR-28

ORIGINAL DATE: 01/03/08

REVIEW/REVISE DATE: 11/19/10, 10/17/13

APPROVAL: Cody L. Phinney, Agency Director

~~~~~~

I. PURPOSE

To assure appropriate use of state systems. This policy is directed at the use of stand-alone, shared or network-attached computers and to provide specific information on inappropriate use of these state owned assets.

II. POLICY

Establishes computer use guidelines on state systems for NNAMHS employees. Abuse of the privilege or violation of this policy may result in disciplinary action up to and including termination.

III. REFERENCES

1. MHDS 3.012 – Replacement of Computer Equipment and Software
2. MHDS 4.040 – Internet Use Policy
3. MHDS 4.068 – Email Use Policy
~~~~~~

4. MHDS Information Technology Security Standard 7.002 – Password Standards
5. NNAMHS Internet Use Policy NN-HR-30
6. NNAMHS E-Mail Use Policy NN-HR-29
7. DHHS Prohibitions & Penalties
8. DoIT Information Technology Security Policy 4.02
9. DoIT Mobile Device Security Policy 54.02

IV. DEFINITIONS

1. Employee: Includes State employees, contractors, students, interns, and residents for which the agency provides State computers.
2. Personal computers include but not limited to desktop computers, notebooks, laptops, and tablet computers.
3. Mobile Device is defined as any handheld electronic device that contains data including but not limited to contact information, E-mail, and/or organizational data, or is capable of connecting with a personal computer (PC), server, or laptop via cable, USB port, or wireless access to transfer data between the two devices. Mobile Devices are information systems as specified in NRS 242.057, and as such are required to meet all laws, policies, and procedures that reference information systems. Example of mobile devices includes smart phones (TREO, Blackberry, iPhone, etc.), notebook (or laptop) computers, and personal digital devices (PDA, iPods, etc.)
4. External hard drives include but not limited to iPods, flash drives, and thumb drives.
5. Protected Individual Information (PII), this includes consumer Protected Health Information (PHI) and employee protected information.

V. PROCEDURE

1. Employee Responsibility for Using State Provided Computers

a. Agency management has a fiduciary responsibility for the protection of State assets, including technology related to the conducting of state business. Each employee has the responsibility to protect the technical assets and data from unauthorized modification, destruction, or disclosure.

b. Employees are responsible to have awareness of information technology security and attend required annual agency training on this subject.

c. Employees are responsible for taking general care of the computer equipment they use. This includes keeping the central processing unit (cpu), monitor, keyboard, and mouse clean.

d. Employees are responsible for backing up files that are stored on their computers local hard drive. The frequency of the backups is based on the criticality and sensitivity of the data along with the acceptable length of non-availability time of the IT resource and data. The backup frequency should not exceed 15 business days.

2. Inappropriate Use of Computer Hardware

a. Use of non-state owned personal computers is prohibited at NNAMHS. (See MHDS Internet Use Policy 4.040, section V, number D; and MHDS E-Mail Use Policy 4.068, section VI, number D)

b. Use of non-state issued external hard drives in state owned computers. This includes devices such as iPods, thumb drives, and flash drives.

c. Storing protected individual information on external hard drives that are not encrypted is prohibited.

d. Use of a state owned notebook to access sensitive protected information via an unsecured wireless location (i.e. WI-FI hotspot, etc.) without encryption or a state provided virtual private network (VPN) connection.

3. Information Technology Department Computer Responsibilities

a. Budget for replacement computers as defined in MHDS Replacement of Computer Equipment and Software, Policy 3.012

b. Budget for new computer equipment and software as needed.

c. Provide technical support in a timely manner to troubleshoot computer hardware, software, and connectivity issues.

d. Provide annual information technology security awareness training.

e. Backup of data stored on the agency's file servers is the responsibility of system administrator.

4. Other

a. Supervisors with concerns about an employee's inappropriate computer use on state systems must request a review in writing to the Agency Director.

b. Employees that have concerns about another employee's inappropriate computer use on state systems should report these concerns to their immediate supervisor. The supervisor will then request a review in writing to the Agency Director.

c. The Agency Director will report suspected violations to the DPBH Information Security Officer.