



**Northeast Montana Health Services
MANAGEMENT INFORMATION
SYSTEMS
POLICIES & PROCEDURE**

This policy supersedes and replaces any previous policies of a like nature.

NEMHS INFORMATION SYSTEMS

Table of Contents

Policy/Procedure	PAGE
MIS 101 . User Workstation Standards	1
1.0 Responsibilities.....	1
2.0 Hardware Configuration Standards.....	1
3.0 Software Configuration Standards.....	2
4.0 Passwords..... ,	3
MIS101 Exhibit 1 - Workstation Configuration Worksheet.....	4
MIS 101 Exhibit 2-NEMHS Password Log.....	7
MIS 101 Exhibit 3 - Monitoring & Configuring Computer or Workstation Set Up Check List	8
MIS 101 Exhibit 4 . Request for Configuration of Restricted Software or Application.....	9
MIS 101 Exhibit 5 . Request for Password Change	10
MIS 101 Exhibit 6 . Separation/Termination Procedures Checklist for Supervisor and IS Department	11
MIS 101 Exhibit 7 . Portable Equipment Issued/Returned.....	13
MIS 102 . Use Of Personal Software.....	1
1.0 Responsibilities	1
2.0 Procedures	1
MIS 102 Exhibit 2-Software Approval Form	3
MIS 103 . Computer Security Incident Reporting	1
1.0 Computer Incident Report.....	1
MIS103 Exhibit 1- Computer Security Incident Report	3
MIS 104. Control of Computer Virus Programs	1
1.0 Responsibilities	1
2.0 Definition of A Computer Virus.....	1
3.0 Virus Symptoms	2
4.0 Virus Prevention Procedures	2
5.0 Virus Eradication.....	3
MIS 105. Computer User I Staff Training Plan	1
1.0 MIS Training and Certification For Support Technicians.....	1
2.0 MIS LAN User Training	1
3.0 E-Mail Training.....	2
4.0 Software Applications	2

MIS 106. Internet Usage Policy.....1

- 1.0 Acceptable Use.....1
- 2.0 Inappropriate Use.....2
- 3.0 Security.....3
- 4.0 Penalties.....3
- 5.0 User Compliance3
- MIS106 Exhibit 1- Computer and Internet Usage Policy4

MIS 107. Electronic Mail Policy.....

- 1.0 Electronic Mail and NEMHS1
- 2.0 General Guidelines.....2
- 3.0 Disciplinary Action.....3

MIS 108. Computer Support Center 1

- 1.0 Overview 1
- 2.0 Operations.....1
- MIS108 Exhibit 1- System Trouble Report Worksheet.....3

MIS 109. Control of Computer Spyware, Adware and SPAM 1

- 1.0 Responsibilities.....1
- 2.0 Definitions.....1
- 3.0 Symptoms.....1
- 4.0 Prevention Procedures.....2
- 5.0 Eradication2
- MIS109 Exhibit 1 -NEMHS Equipment Relocation Control Log..... .4
- MIS109 Exhibit 2 - Information Technology Equipment Sanitization Record..... .5

Finance P&P: Information Systems
SOP#MIS101 Revision:REV. 2
Effective Date: _____

Prepared by: _____
CFO Approval: _____
CEO Approval: _____

Title: MIS101 USER WORKSTATION STANDARDS

Policy: Personal computer workstations represent one of the most significant NEMHS fiscal investments. Enforcement of a consistent configuration is required to ensure maximum use of these assets. All NEMHS user workstations shall maintain a consistent hardware and software configuration as delineated in this document.

Purpose: To delineate specific standards regarding the configuration of NEMHS personal computer workstations.

Scope: This policy applies to all NEMHS personnel computer systems.

Procedure:

1.0 RESPONSIBILITIES

- 1.1 INFORMATION SYSTEMS MANAGER - The Information Systems Manager is ultimately responsible for enforcing this standard. The IS Manager shall regularly review these guidelines and ensure workstation configuration standards support current technology and user requirements.
- 1.2 DEPARTMENT MANAGER - The Department manager shall be responsible for monitoring and enforcing workstation configuration standards. The IS Manager is responsible for the proper installation and configuration of approved software.
- 1.3 WORKSTATION USERS - All workstation users shall adhere to the configuration guidelines. Deviation from these standards shall be coordinated with the Information Systems Department through the user's department manager. Users shall notify the IS Department of any variances from this policy.

2.0 DESKTOP HARDWARE CONFIGURATION STANDARDS

2.1 New user workstations shall meet the following minimum standards:

CPU	Pentium 4 or greater
Bus type	PCI
Cache	512KB
Memory	512MB
Hard Drive	80.0 GB EIDE Ultra
Floppy Drive	One 3.5 inch 1.44 MB or Card Reader(USB)
CD-ROM	CDRW/DVD (combo drive)
Mouse	PS-2 Type or USB
Printer Ports	One ECP capable or USB 2.0

Video	SVGA, 128 MB Video RAM (shared)
Monitor	17 or 19 inch, LCD
Network Interface	PCI 10/100/1000 MB Ethernet
USB Ports	2 or more

- 2.2 Only personnel from the Information Systems Department shall install and configure user workstation hardware. A Computer or Workstation Configuration Record (MIS Exhibit 1) will be completed on all existing hardware and on new hardware as purchased. The Monitoring & Configuring Computer or Workstation Set up Checklist (MIS 101 Exhibit 3) will also be completed by the IS Department on all new purchases.
- 2.3 Requirements that exceed these standards shall be addressed on a case-by-case basis. All special configuration requirements shall be coordinated through the Information Systems Department.

3.0 SOFTWARE CONFIGURATION STANDARDS

- 3.1 AU user workstations shall only use software approved by the Information Systems Department.
- 3.2 New user workstations shall be configured with the following software.

Category	Authorized Software
Operating System	XP Professional or Latest
Office Automation	
Word Processing	Word (2000 or newer)
Spreadsheet	Excel (2000 or newer)
Presentation Graphics	Power Point
Personal Database	Access (2000 or newer)
Internet Browser	Internet Explorer (5.5 or above)
Electronic Mail	Outlook (2000 or newer)
Personal Scheduling	Schedule+/Outlook (2000 or newer)

- 3.3 Only personnel from the Information Systems Department shall install and configure software on user workstations. Requests for software not listed above shall be made on the Request for Configuration of Restricted Software or Application (MIS 101 Exhibit 4) and forwarded to the IS Department for consideration. Requests for approved software may be made on the NEMHS Software Approval Form (MIS 102 Exhibit 1).
- 3.4 Requirements that exceed these standards shall be addressed on a case-by-case basis. All special configuration requirements shall be coordinated through the Information Systems Department. User shall submit MIS 102 Exhibit 1 - NEMHS Software Approval Form to the IS Department for consideration.

4.0 PASSWORDS

- 4.1 The IS Department will have the end user set up their own passwords for computer access and Screen Saver logoffs on all computers. Program access passwords will be set up as required.
- 4.2 Passwords may only be changed by the end user. The IS Department will be able to reset all passwords for accessing software and applications in such a case as a password has been forgotten. (MIS 101 Exhibit 2-Password Log)
- 4.3 Passwords are required to be changed semi-annually, and the the IS Department has a schedule to notify users to enter new password. Should passwords need changing sooner (terminations, security compromises), personnel shall complete a Request for Password Reset. (MIS 101 Exhibit 5)
- 4.4 Personnel shall keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts. The IS Department will not log user passwords.
- 4.5 Requests for equipment are to be made by Supervisors to the IS Department. If portable equipment is issued to an employee of NEMHS, a Portable Equipment Issued/Returned form (MIS Exhibit 7) will be completed as per the instructions on the form. Return of equipment at termination or separation is accomplished on the same form.
- 4.6 At the termination or separation of an employee, the Department Supervisor will initiate the Separation/Termination Procedures Checklist (MIS 101 Exhibit 6) and forward it to the IS Department for completion of sanitization of all equipment used by the terminated employee.

Revision History:

Revision	Date	Description of changes	Requested By
0	3/2/05	Initial Release	
1	5/26/05	I.S. Manager Review	
2	10/26/06	Edit 4.1,4.2,4.3 Passwords	

**MIS101 EXHIBIT 1 COMPUTER OR WORKSTATION
CONFIGURATION RECORD**

Department: _____ **User:** _____ **Computer Description:** _____
A. System Identification: _____

Component	Manufacturer	Model	Property #	Serial Number
CPU				
Monitor				
Printer				
Other:				

B. Hardware Components

Component	Manufacturer	Model
Floppy Drive		
Mouse/Pointing Device		
Hard Drive 1		
Hard Drive 2		
CD-ROM Drive		
Tape Drive		
Video Card		
Sound Card		
Network Interface Card		
Disk Controller		
USB 1.1 or 2.0		
Other		

C. Hardware Configuration

1. CPU Type: _____ Clock Speed: _____
 2. System BIOS: _____
 Manufacturer: _____ PNP: YES NO
 BIOS Date: _____ BIOS Revision: _____

3. Memory

RAM Type: _____ RAMCapacity: _____

4. Automatic Logoff (ie: passworded screen saver): _____

5. User and/or Supervisor Passwords _____

6. Antivirus: _____

7. Resource Assignments: _____

Component	IRQ	Base I/O	Base Memory	DMA
COM1				
COM2				
MOUSE				
LPT1 or USB				
Disk Controller				
Video Controller				
Sound Card				
Network Interface				
Modem				
Other				

D. Software Configuration

Software	Vendor	Version/Revision	License ID
Operating System			
Word Processing			
Spreadsheet			
Presentation Graphics			
Database			
Electronic Mail			
Internet Browser			
Security			
Anti-Virus			

E. Network Configuration

Resource	Primary IP Address	Secondary IP Address	Comments
DNS			
Gateway			
NIC/Machine IP		N/A	
WINS OR Net Bios			
Subnet IP			

**MIS 101 EXHIBIT 3
MONITORING & CONFIGURING
COMPUTER OR WORKSTATION SET UP CHECK LIST**

DATE _____ **Prepared By:** _____

Computer Location _____

Outlook

_____ **Email account**

_____ **Security**

_____ **Disclaimers**

Anti-Virus

_____ **Scan hard drive**

Passwords - updated

Spyware - updated

Check for Unauthorized Programs

Disk Clean up

Notes (What was done, problems encountered, etc.):

MIS 101 EXHIBIT 4
NEMHS REQUEST FOR CONFIGURATION OF
RESTRICTED SOFTWARE OR APPLICATION

Date _____ **Requested by** _____

Software or Application Needed: _____

Purpose: _____

Time Of Date Needed: _____

Length of Time Needed: _____

IS DEPARTMENT USE	
Approved by:	
Denied by/Reason:	
Date Installed:	By:
Date Removed:	By:
Supervisor Signature:	

**MIS 101 EXHIBIT 5 NEMHS
REQUEST FOR PASSWORD RESET**

Date: _____ **Requested by:** _____

Reason for request _____

IS DEPARTMENT USE:

Password Reset by: _____

Date: _____

Entered in Log: _____

MIS 101 EXHIBIT 6

NEMHS SEPARATION/TERMINATION PROCEDURES CHECKLIST FOR SUPERVISOR AND IS DEPARTMENT

Supervisor: Check all that apply to the terminating employee. Determine passwords used by employee. Collect any portable equipment issued to terminating employee (example: cell phone, laptop, pager) and complete the Portable Equipment Issued/Returned Form (MIS 101 Exhibit 7). Forward along with this form to the IS Department for completion.

IS Department: Complete needed clean up and record new access codes and passwords in IS Department Log (NOT ON THIS FORM). Copy form for IS department records, forward original to HR Department.

Terminating Employee Name _____

Date of Termination _____ Department _____

Network access account (network, mainframe, servers, etc.)

User ID _____ Password _____

IS: ID & Passwords Changed/Deleted New Recorded in Log

E-mail account

User ID _____ Password _____

Should email be rerouted? If so: User ID:

IS: ID & Passwords Changed Deleted New Recorded in Log

E-mail rerouted

Computer

Type/Serial Number _____ User Access Code _____

IS Access Code Changed Deleted New Recorded in Log

Laptop

Type/Serial Number _____ User Access Code _____

IS Access Code Changed Deleted New Recorded in Log

Printer (laser, inkjet, all-in-one)

Type/Serial Number _____ User Access Code _____

Fax and/or copier

Type/Serial Number _____ User Access Code _____

Cell phone and accessories

Type/Serial Number _____ Phone # _____

Access Code (voice mail) _____

IS: Equipment Relocated to _____

pager

Type/Serial Number _____ Phone # _____

Access Code _____

IS: Equipment Relocated to _____

Projector Type/Serial Number _____

- Voice mail Access Code
 IS: Message cleared/changed to _____ Calls to be rerouted to reroute New
 access code recorded in Log Telephone access
 Access Code _____
 IS: Deleted New access code recorded in Log
- VPN connection access
 Access Code _____
 IS: Deleted New access code recorded in Log
- Company-provided dial-up account access
 Access Code _____
 IS: Deleted New access code recorded in Log
- Cancel specific software access (accounting software, HR software, etc.)
 Supervisor-List and include access codes:

IS Access codes changed/deleted on following:

Employee was authorized purchaser with following vendors:

IS: Contact suppliers and vendors to cancel employee as authorized purchaser

Supervisor Signature: _____ **Date:** _____

IS Department Signature: _____ **Date:** _____

Finance P&P: Information Systems
SOP # MIS102 Revision:REV.1
Effective Date:_____

Prepared by:_____
CFO Approval:_____
CEO Approval:_____

Title: MIS 102 USE OF PERSONAL SOFTWARE

Policy: NEMHS provides its employees with a state of the art computing environment. To ensure the efficiency and supportability of NEMHS computing resources strict software configuration control procedures are required. The use of personally owned, unlicensed or unauthorized software on NEMHS computing assets is prohibited.

Purpose: To delineate specific guidelines regarding the use of personal software on NEMHS computing assets.

Scope: This policy applies to all NEMHS personnel and computer systems.

Procedure:

1.0 RESPONSIBILITIES

- 1.1 The NEMHS Information Systems Manager shall manage the configuration control of all NEMHS computing resources. The Information Systems Manager shall act as approval authority for all requests to use personal software.
- 1.2 Department Managers shall enforce this policy. Department Managers shall forward requests for the use of personal software to the Information Systems Manager for approval.
- 1.3 NEMHS users shall follow the guidelines of this policy document. Users shall seek and receive approval prior to using personal software on NEMHS computing assets. Requests should include proof of a valid license and the original diskettes which will be kept by the NEMHS Information Systems Manager. If unauthorized software is found or suspected users shall immediately notify their Department Manager. Users shall not take any action to eradicate or remove the software.
- 1.4 Department managers shall monitor the use of personal or unauthorized software and report violations to the Information Systems Manager. When illegal software is suspected or detected, the IS Manager shall coordinate all actions required to eradicate the software and return the system to the approved configuration.

2.0 PROCEDURES

- 2.1 The NEMHS has provided a Common Operating Environment (COE) for all users. This common operating environment provides the most commonly used applications required for normal business operations. However in some cases the need may arise for software solutions outside the normal scope of the NEMHS COE.
- 2.2 When this requirement is identified the user shall formally request permission to use the personal software program. A completed MIS 102 Exhibit 1 — NEMHS

Software Approval form shall be forwarded via the user's Department Manager to the Information Systems Manager.

- 2.3 The Information Systems Manager shall evaluate all requests for the use of personal software. Prior to approving the software for use, the IS Manager shall ensure that the application has been tested for interoperability with the NEMHS COE. Should the application fail to run in the NEMHS COE the request shall be rejected unless a critical business need is identified and hardware upgrade can accommodate the request.
- 2.4 All freeware, shareware, games or entertainment software of any kind are forbidden at all times and may not be introduced, loaded, stored or executed in any fashion on any NEMHS computing resources or personally owned computing devices that are attached to The NEMHS network.
- 2.5 All forms of sexually related materials, entertainment software or pictures of any kind of sexual nature are forbidden at all times and may not be introduced, loaded, stored or executed in any fashion on any NEMHS computing resources or personally owned computing devices that are attached to The NEMHS network.

Revision History:

Revision	Date	Requested By
0	3/2/05	
1	5/26/05	I.S. Manager Review

MIS 102 EXHIBIT I NEMHS SOFTWARE APPROVAL FORM		
Software Requested:		
License Code:		
Department Requesting:		Date:
Purpose:		
User:		
Approved by:	Rejected by:	Date:
Installed by:	Date:	
Notes:		

Finance P&P: Information Systems
SOP # MIS103 Revision:REV.2
Effective Date: _____

Prepared by: _____
Approval CFO: _____
Approval CEO: _____

Title: MIS103 = COMPUTER SECURITY INCIDENT REPORTING

Policy: Computer and data processing security procedures are intended to provide for the reporting, documenting and investigating of all incidents, which constitute a threat to the secure operation of NEMHS data processing assets. A Computer Security incident is an instance of unauthorized use (accidental or intentional), loss, disclosure, modification, or destruction of data processing equipment software or NEMHS data assets. All incidents of this nature are to be reported no matter how trivial.

Purpose: This policy specifically details the communication procedure for reporting any incident or suspected security incident.

Scope: This policy applies to all remote data terminal sites, desktop computers, data centers, telecommunications facilities, as well as all data, software, hardware and personnel involved in automatic data processing.

Procedure:

1.0 COMPUTER INCIDENT REPORT

- 1.1 Any employee who knows or suspects a security violation has occurred shall expeditiously initiate an incident report (MIS 103-Exhibit 1). The incident will be documented on the attached form and forwarded to the Information Systems Manager. The report may be delivered by electronic mail, interoffice mail or hand delivered.
- 1.2 At no time will employees that report a real or perceived security incident be subjected to retaliatory action. However, those who file fraudulent security incidents will be subject to disciplinary action and/or termination.
- 1.3 Security incident reports will be evaluated and investigated by the Information Systems Manager to determine the severity of the compromise and the scope of any follow up action that may be required.
- 1.4 The Information Systems Manager will immediately notify the Chief Financial Officer (CFO) and HIPPA Compliance Officers of the occurrence of any security violation.
- 1.5 Reported incidents will be documented and retained for a period not less than three years or as long as required by NEMHS auditors or insurance regulators.
- 1.6 The Information Systems Manager will document verified security breeches in detail and recommend additional countermeasures, safeguards and procedural changes required to reduce the risk of a re-occurrence of the threat or incident.

Revision History:

Revision	Date	Description of changes	Requested By
0	3/2/05	Initial Release	
1	5/26/06	I.S. Manager Review	
2	10/26/06	Update Font & Added Resolution	

MIS 103 EXHIBIT 1 COMPUTER SECURITY

INCIDENT REPORT

Office Code: _____ Phone: _____

To: Information Systems Manager

A computer security incident was detected / observed / discovered on
(date/time): _____ at(location): _____

System Identification:

System Description: _____

Software Systems Involved: _____

Type of Security Incident:

The nature of this security incident was: (Check all that apply):

- Unauthorized access to computing resources
- Unauthorized disclosure or use of personal password
- Improper use of computing resources
- Alteration of data or computer systems
- Other: (Explain) _____

Sensitivity of Data:

- Not sensitive - Routine correspondence of little detrimental value
- Business Confidential - Proprietary Data
- Business Sensitive — Financial Data
- Business Sensitive - Personnel Related Data
- Business Sensitive - Other

Impact of Security Incident

The effect of the security violation included the following: (Check all that apply)

- Disclosure of Data
- Destruction or modification of data or systems
- Denial of service
- Other: (Explain on separate sheet)

Personnel Involved: (List all involved personnel. Use additional sheets if required.)		
Name :	Location:	Computer ID Number:

Incident Description: Describe incident details using a separate sheet if required.

Resolution: _____

Dept. Mgr.: _____ **Notified Date:** _____

Finance P&P: Information Systems
SOP # MIS104 Revision:REV.1
Effective Date: _____

Prepared by: _____
CFO Approval: _____
CEO Approval: _____

Title: MIS104 CONTROL OF COMPUTER VIRUS PROGRAMS

Policy: Computer viruses are unauthorized programs that are capable of self-propagation. This type of software program is almost always destructive and normally results in loss of data

Purpose: To define NEMHS policy regarding the prevention of loss of data resulting from an outbreak of a computer virus. This policy further delineates actions required to recover from a virus attack on NEMHS computing assets.

Scope: This policy applies to all NEMHS personnel and computer systems.

Procedure:

1.0 RESPONSIBILITIES

- 1.1 Training will be coordinated with the Department Managers. The Information Systems Manager shall be responsible for training Department Managers on computer virus control. Department Managers are responsible for training users in their respective departments. The Information Systems Manager shall develop virus control procedures and train other Information Systems Department personnel. Additionally, the IS Manager shall be responsible for evaluating and updating appropriate computer virus detection software.
- 1.2 IS Manager shall coordinate actions required to prevent computer virus outbreaks. When a computer virus is suspected or detected, the IS Manager shall be notified using NEMHS MIS 108 - Exhibit 1. The IS Manager shall organize all actions required to eradicate the virus and recover user data to the greatest extent possible.
- 1.3 Users shall follow the guidelines of this policy document. When a computer virus is suspected, users shall immediately notify IS Manager and the Department Manager. Users shall not take any action to eradicate or recover from the virus attack.

2.0 DEFINITION OF A COMPUTER VIRUS

- 2.1 Computer viruses are very small pieces of software that attach themselves to legitimate software. When the legal software is executed, the virus code is executed and carries out the destructive purpose of the virus.
- 2.2 Virus software can be created to execute immediately or at a pre-planned sequence of events or time. The classic example is a virus that is set to cause deletion of key system files on a specific date such as Friday the 13th.
- 2.3 Virus programs create unwanted system activity that almost always has destructive results. Results of a virus attack can include the following:

- Corrupt or overwritten boot sector of a disk
- Corrupt data files
 - Sudden reformatting of the hard drive
 - Corrupt file allocation tables or file system data structures
- Corrupt key system or applications software.

3.0 VIRUS SYMPTOMS

3.1 Symptoms of a computer virus attack include the following:

An unexpected or unwanted message on the screen

- Unexplained increase in file sizes
 - Increase in the number of bad disk sectors
- Major changes in system performance
- Corruption of data files
- Failure of applications software that previous worked correctly
- Warning by computer virus detection software

3.2 Users detecting any of these symptoms should immediately contact the IS Manager and notify their department manager for further investigation. Users shall not troubleshoot suspected virus attacks.

4.0 VIRUS PREVENTION PROCEDURES

- 4.1 Only software specifically authorized by the Information Systems Department shall be installed on NEMHS computer systems.
- 4.2 Only personnel from the Information Systems Department shall be allowed to install and configure software on NEMHS systems.
- 4.3 Commercially available computer protection software shall be installed on all NEMHS computer systems. Only virus detection software approved by the International Computer Security Association (formally NCSA and now ICSA Labs a division of TruSecure Corporation) shall be selected for installation on NEMHS systems.
- 4.4 Virus detection software shall also be integrated with system backup software in order to ensure routine backups include virus scans. Should a virus be detected during system backup then an attempt to clean the file shall be initiated. Should the attempt to clean the file fail, then the file shall be quarantined and a message recorded in the backup log.
- 4.5 Users shall receive training, at least semi-annually, on computer security policy including virus prevention. This training session shall also include indoctrination into how to operate the computer virus protection software installed on their system. Users shall be trained in how to scan for viruses. Only Information Systems Department personnel shall carry out virus recovery procedures.

- 4.6 All software shall be scanned for viruses before installation.
- 4.7 All floppy diskettes shall be scanned before use. Virus detection software installed on user workstations and file servers shall be configured to scan floppy disks before accessing data from these drives.
- 4.8 Internet Search Engines shall be used to search the Internet.

5.0 VIRUS ERADICATION

All NEMHS computing assets shall have an ICSA approved virus detection software program installed at all times. Each of these programs is updated routinely. The Information Systems Staff shall ensure that the most up to date version of this software is available for users.

Revision History:

Revision	Date	Description of changes	Requested By
0	3/21/05	Initial Release	
1	5/26/06	I.S. Manager Review	

Finance P&P: Information Systems**SOP # MIS106 Revision:REV.2****Effective Date:** _____**Prepared by:** _____**CFO Approval:** _____**CEO Approval:** _____**Title: MIS106 INTERNET USAGE POLICY**

Policy: Access to the Internet through the NEMHS computer network is a privilege. Users granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. Users who violate the provisions outlined in this document are subject to disciplinary action up to and including termination. In addition, any inappropriate use that involves a criminal offense will result in legal action. All users are required to acknowledge receipt and understanding of guidelines contained in this document.

Purpose: To define policies and procedures for access to the Internet through the NEMHS network infrastructure.

Scope: This policy applies to all personnel with access to Internet and related services through the NEMHS network infrastructure. Internet Related services include all services provided with the TCP/IP protocol, including but not limited to World Wide Web (WWW) access.

Note: Electronic Mail (e-mail) is addressed separately in MIS 107.

Procedure:**1.0 ACCEPTABLE USE**

- 1.1 Access to the Internet is specifically limited to activities in direct support of official NEMHS business.
- 1.2 In addition to access in support of specific work related duties, the NEMHS Internet connection may be used for educational and research purposes.
- 1.3 If any user has a question of what constitutes acceptable use he/she should check with their supervisor for additional guidance. Management or supervisory personnel shall consult with the Information Services Manager for clarification of these guidelines.
- 1.4 All Internet data that is composed, transmitted, or received via NEMHS computer systems is considered to be part of the official records of NEMHS and, as such are subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in electronic transmissions is accurate, ethical, appropriate and lawful.
- 1.5 The equipment, services, and technology provided to access the Internet remain at all times the property of NEMHS. As such, NEMHS reserves the right to monitor Internet traffic, retrieve and read any data composed, sent or received through our online connections and stored in our computer systems.

- 1.6 Loading of some programs can have detrimental effects on personal computers, network system, and Internet connections and speed. Examples of Restricted Applications:

- 3rd Party Screensavers
- Internet Video (Web Casts, Streaming Video, Shockwave, Digital Music)
- Live Weather Reporting (Weather Bug)
- MP3 Downloads (Music Format, Audio)
- Webcasts

The above programs must be pre-approved and installed by the IS Technology Coordinator.

Examples of Unauthorized Applications:

- Webshots Desktop Software
- Lycos
- Unauthorized Screen Print Utilities
- Comet Cursors
Sports and Stock Tickers (Real Time)
- Chat Software (Chat Rooms, Yahoo, Messengers)
- Internet Radio (Radio Stations with Streaming Audio)
- Internet Gaming (Games played on-line real time)
- Internet Movies
- Demonstration Software
- Real Time Messenger services (MSN Messenger, Yahoo Messenger)

Note: The above examples are not all inclusive.

2.0 INAPPROPRIATE USE

- 2.1 The NEMHS Internet access shall not be used for any illegal or unlawful purposes. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials.
- 2.2 The NEMHS Internet access shall not be used for private, recreational or other non-NEMHS related activity.
- 2.3 The NEMHS Internet connection shall not be used for commercial or political purposes.
- 2.4 Use of the NEMHS Internet access shall not be used for personal gain such as selling access of a NEMHS user login. Internet access shall not be used for or by performing work for profit with NEMHS resources in a manner not authorized by NEMHS.
- 2.5 Users shall not attempt to circumvent or subvert security measures on the NEMHS's network resources or any other system connected to or accessible through the Internet.
- 2.6 NEMHS users shall not use Internet access for interception of network traffic for any purpose unless engaged in authorized network administration.

2.7 NEMHS users shall not make or use illegal copies of copyrighted material, store such copies on NEMHS equipment, or transmit these copies over the NEMHS network.

3.0 SECURITY

3.1 NEMHS users who identify or perceive an actual or suspected security problem shall complete a Computer Security Incident Report (MIS102-Exhibit 1) and immediately contact the NEMHS Information Systems Security Manager.

3.2 Users shall not reveal account password or allow another person to use their account. Similarly, users shall not use the account of another user.

3.3 Access to NEMHS network resources shall be revoked for any user identified as a security risk or a demonstrated history of security problems.

4.0 PENALTIES

Any user violating these policies or applicable state, or federal laws is subject to the loss of network privileges and any other NEMHS disciplinary actions deemed appropriate. Inappropriate use that involves a criminal offense will result in legal action.

5.0 USER COMPLIANCE

5.1 All terms and conditions as stated in this document are applicable to all users of the network and the Internet connection. These reflect an agreement of all parties and should be governed and interpreted in accordance with the laws of the State of Montana and any applicable Federal laws.

5.2 All users must agree to abide by this policy by signing the Acknowledgement of Receipt and Understanding form Exhibit 1 - Computer and Internet Usage Policy

Revision History:

Revision	Date	Description of changes	Requested By
0	3/2/05	Initial Release	
1	5/26/06	I.S. Manager Review	
2	10/26/06	Update Fonts	

MIS106 EXHIBIT 1 COMPUTER AND INTERNET USAGE POLICY

ACKNOWLEDGEMENT OF RECEIPT AND UNDERSTANDING

Access to the Internet through the NEMHS is a privilege. Users granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. Users who violate the provisions outlined in this document are subject to disciplinary action up to and including termination. In addition, any inappropriate use that involves a criminal offense will result in legal action. All users are required to acknowledge receipt and understanding of guidelines contained in this document.

ACCEPTABLE USE

Access to the Internet is specifically limited to activities in direct support of official NEMHS business but may be used for educational and research purposes. If any user has a question regarding acceptable use he/she should check with their supervisor for additional guidance. Management or supervisory personnel shall consult with the Information Services Manager for clarification of these guidelines.

All Internet data that is composed, transmitted, or received via NEMHS computer systems is considered to be part of the official records of NEMHS and, as such are subject to disclosure to law enforcement or other third parties consequently, employees should always ensure that the business information contained in electronic transmissions is accurate, ethical, appropriate and lawful.

The equipment, services, and technology provided to access the Internet remain at all times the property of NEMHS. As such, NEMHS reserves the right to monitor Internet traffic, retrieve and read any data composed, sent or received through our online connections and stored in our computer systems.

INAPPROPRIATE USE

The NEMHS, Internet access shall not be used for any illegal or unlawful purposes. Examples include the transmission of violent, threatening, defrauding, pornographic or obscene materials.

Use of the Internet World Wide Web (www) shall be used for the conduct of NEMHS business only.

Use of NEMHS electronic mail is intended to be used for the conduct of NEMHS business only. Personal email accounts may not be linked to NEMHS equipment. These services shall not be used to harass, intimidate or otherwise annoy another person or for private, recreational or other non-NEMHS related activities including commercial or partisan political purposes or for personal gain such as selling access of a NEMHS user login. Internet access shall not be used for performing work for profit with NEMHS resources in a manner not authorized by The NEMHS.

Users shall not attempt to circumvent or subvert security measures on either the NEMHS network or any other system connected to or accessible through the Internet. NEMHS users shall not use Internet access for interception of network traffic for any purpose unless engaged in authorized network administration.

NEMHS users shall not make or use illegal copies of copyrighted material, store such copies on NEMHS equipment, or transmit these copies over the NEMHS network. This includes copies of software that the NEMHS has not purchased or does not have a license.

INTERNET AND EMAIL ETIQUETTE

NEMHS employees shall ensure all communication through NEMHS e-mail or messaging services is conducted in a professional manner. The use of vulgar or obscene language is prohibited. NEMHS users shall not reveal private or personal information without specific approval from management.

Users should ensure that e-mail messages are sent to only those users with a specific need to know. Emails must include appropriate disclaimer captions as set forth in MIS 107-3.4.

The transmission of e-mail to large groups or messages with large file attachments should be avoided. Users should note **Electronic Mail is not guaranteed to be private. Messages transmitted through the NEMHS e-mail system or network infrastructure are the property of NEMHS and are therefore subject to inspection and control.**

SECURITY

NEMHS users who identify or perceive an actual or suspected security problem shall immediately contact the NEMHS Information Systems Security Manager. Users shall not reveal account password or allow another person to use their account. Similarly, users shall not use the account of another user. Access to NEMHS network resources shall be revoked for any user identified as a security risk or for those with a demonstrated history of security problems.

USER COMPLIANCE

All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with Federal and State of Montana laws. Any user violating these policies or the applicable state, or federal laws is subject to the loss of network privileges and any other NEMHS disciplinary actions deemed appropriate.

I understand and will abide by the *NEMHS Management Information System Policies & Procedures*. I further understand that any violation of this policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, disciplinary action and or appropriate Legal action may be taken. I have received a copy of this policy.

User Signature _____ Date _____

Supervisor Signature _____ Date _____

Finance P&P: Information Systems
SOP # MIS107 Revision:REV.2
EffectiveDate: _____

Prepared by: _____
CFO Approval: _____
CEO Approval: _____

Title: **MIS107 ELECTRONIC MAIL POLICY**

Policy: Electronic mail (e-mail) is a powerful tool that greatly enhances productivity and communication within NEMHS. The use of this capability shall be limited in scope to support the business needs of NEMHS. Information system resources are shared among users, inappropriate use by users may interfere with the use of information system resources of another. This policy is intended to protect the integrity of NEMHS information system facilities and its users against unauthorized or improper use.

Purpose: To define specific standards regarding the use of electronic mail on NEMHS computing assets.

Scope: This policy applies to all NEMHS personnel and computer systems.

Definitions: User: any person authorized to access NEMHS's e-mail system, including employees, members of the medical staff, independent contractors, consultant, temporary workers, students and other individuals or entities who have access to NEMHS e-mail system.

Procedure:

1.0 ELECTRONIC MAIL AND NEMHS

All portions of the NEMHS information infrastructure including the information being transported by this infrastructure are the property of the NEMHS. This includes all electronic mail transmitted or received through the NEMHS information infrastructure. Since electronic mail is the property of NEMHS, all electronic mail accounts and the electronic mail stored by these accounts are subject to inspection at any time. Electronic mail is a powerful tool that can greatly enhance communication. The use of electronic mail by NEMHS employees is encouraged within the following guidelines.

2.0 GENERAL GUIDELINES

- 2.1 Electronic Mail is not guaranteed to be private. Messages transmitted through the NEMHS e-mail system or network infrastructure are the property of NEMHS and are therefore subject to inspection at any time. As stated in the NEMHS Computer and Internet Usage Policy Acknowledgement, the use of this system shall imply consent to search.
- 2.2 Use of NEMHS electronic mail or messaging services shall be used for the conduct of NEMHS, business only. NEMHS e-mail shall not be used for private, recreational or other non-NEMHS related activity. Personal e-mail is not official business, although minimal use for personal communication is allowed. It is the responsibility of the user to assure that email of a personal nature complies with

this NEMHS policy. Personal e-mail accounts shall not be installed on NEMHS computers.

- 2.3 NEMHS e-mail shall not be used for commercial or partisan political purposes.
- 2.4 NEMHS employees shall ensure all communication through NEMHS e-mail or messaging services is conducted in a professional, legal and ethical manner. The use of vulgar or obscene language is prohibited.
- 2.5 NEMHS users shall not reveal private or personal information without specific approval from management.
- 2.6 Users should ensure that e-mail messages are sent to only those users with a specific need to know. The transmission of e-mail to large groups or messages with large file attachments should be avoided.
- 2.7 NEMHS e-mail shall not be used for any illegal or unlawful purposes. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials. This policy reflects an agreement of all parties and is to be governed and interpreted in accordance with Federal, State and local laws.
- 2.8 NEMHS e-mail services shall not be used to harass, intimidate or otherwise annoy another person.
- 2.9 NEMHS shall not be held liable for damages related to inappropriate use of e-mail by NEMHS employees or their family. Users are responsible for their information systems accounts, and may be held accountable if someone uses their account with permission and violates policy.
- 3.0 Users must use only those information systems resources that NEMHS has authorized for their individual use. Users are authorized to access, use, and copy, modify, or delete files and data on their own account. Users are not authorized to perform any of these functions on another user's account or a NEMHS system.
- 3.1 User privacy is not to be violated. It is the responsibility of the user to protect their privacy. Users should not leave a password where it can be easily found, give a password to someone else, or leave confidential information on a screen where it could be viewed by an unauthorized person, or leave a public PC or terminal signed on and unattended.
- 3.2 Chain e-mail messages are not to be forwarded using any NEMHS resource. Chain e-mail is defined as any message sent to one or more people that ask the recipient to forward it to multiple others and contains some promise of reward for forwarding it or threat of punishment for not doing so.

Chain e-mail messages can have technological, social and legal ramifications. Chain e-mail messages have the ability to clog an entire network and degrade the ability of employees to do their work. Heavy traffic due to chain mail messages can disrupt not only the e-mail service but other network activities as well.

- 3.3 Users may not intentionally obscure, change, or forge the date, time, physical source, logical source, or other label or header information on electronic mail, files or reports.
- 3.4 Information necessary to perform job functions may include information subject to privileged or statutory protection from discover, and that such information must be maintained in accordance with applicable statutory mandates. Users must exercise due care when transmitting information and include the following appropriate captions with each message:

- For general correspondence:

****The information contained in this communication may be of a nature that it must be protected from disclosure. If the reader of this message is not the intended recipient, please notify us immediately by replying to the message and deleting it from your computer.****

For personal e-mails, add:

****This e-mail contains the thoughts and opinions of the sender and does not represent official Northeast Montana Health Services, Inc. policy. The recipient is hereby notified that correspondence to this account is the property of NEMHS and therefore subject to inspection.****

- For patient information: The user shall also ensure that patient information and records are disclosed only in accordance with applicable state and federal laws and regulations and NEMHS policy and procedures:

****The information contained in this communication is PRIVILEGED AND CONFIDENTIAL and is for the use of the intended individual or entity. This information is the property of the entity sending the information. If the reader of this message is not the intended recipient, you are hereby notified that any use, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by replying to this message and deleting it from your computer.****

3.5 Transmission of Patient Health Information (PHI) will occur over point-to-point connections using dial-up lines, which does not require encryption and has a very small probability of interception, or can be sent using NEMHS mail using encryption software such as Centurion Mail. Any transmission over "open networks", e.g. Internet transmissions, will employ the use of a secure site (with login and password) or the use of an acceptable encryption method. Refer to the HIPPA Acceptable Encrytion policy.

3.0 DISCIPLINARY ACTION

Failure to follow the guidelines of this document will result in disciplinary action up to and including termination. NEMHS reserves the right, without notice to temporarily limit or restrict any individual's use and to inspect, copy, remove, or otherwise alter any data, file, or system resource, which may undermine the authorized use of any information systems facility.

Revision History:

Revision	Date	Description of changes	Requested By
0	3/1/05	Initial Release	
1	5/26/06	I.S. Manager Review	
2	10/26/06	3.5 Add Encryption Software	

Finance P&P: Information Systems

SOP # MIS108 Revision:REV.2

Effective Date: _____

Prepared by: _____

CFO Approval: _____

CEO Approval: _____

Title: MIS108 - COMPUTER SUPPORT SERVICE**Policy:** Maintain IS support for all departments in the NEMHS.**Purpose:** To provide cost effective staffing, training and logistics for an effective support department. Identify staffing, training, and logistic requirements for an internal service/support center.**Scope:** Provide technical support to all departments of NEMHS with all Information Systems needs including:

Hardware support - assistance with installation, usage, upgrades or failures of all Information Technology related computer and communication equipment.

Software support - assistance with technical questions on all COE Operating system, email, application and database software.

1.0 OVERVIEW

- 1.1 Determine the requirements of support services by assessing the needs of the user and NEMHS.
- 1.2 Develop a mission statement such as "To increase the NEMHS productivity by providing a single point of contact and responsibility for rapid resolution of information systems problems.
- 1.3 Integrate the Computer Support Services into NEMHS Information Systems framework to ensure that service is accessible to NEMHS users.
- 1A Develop guidelines and procedures that outline response rates, priority levels, staffing requirements, customer satisfaction and summary reports to planning committees that will serve as the voice of the users.
- 1.5 Employees shall contact their Supervisor when support services are needed. The Supervisor will complete the System Trouble Report Worksheet (MIS 108 Exhibit 1) and forward it to the IS Department for resolution.

2.0 OPERATIONS

- 2.1 Assign Customer Service/Support Manager - duties include defining the scope of the Support Service, forecasting the quantity of trouble reports to determine the size of the Service Center staff, and creating instructions, procedures, equipment requirements and schedule requirements.
- 2.2 Develop organizational procedures - duties to include aligning customer service staff with the structure of NEMHS, developing tiers of support expertise, prioritizing trouble reports and allocating trouble report, phone request, and email requests to the appropriate staff.

- 2.3 Determine location requirements - identify the location of personnel assigned to NEMHS, determine the need for remote staffing and create remote helpdesk procedures and equipment needs/requirements. Determine procedures for lab troubleshooting.
- 2.4 Determine staffing and training requirements for Service/Support Personnel - Outline schedules, on call procedures, and standard training procedures that define the expectations and responsibilities of support personnel. Develop a career pipeline for advancement within Customer Service/Support or further areas of growth. Plan for scheduled training and attendance at technical conferences. Assign additional duties to promote growth and teamwork.
- 2.5 Staff the Service/Support Center - work with Human Resources within the IS department to find qualified IS personnel.
- 2.6 Analyze the quality of support - define random or scheduled customer satisfaction surveys and update procedures and policies based on feedback received.
- 2.7 Update the Service/Support center - evaluate the needs of the NEMHS and develop annual reviews to ensure the Service Support center continually meets the technology needs of NEMHS.

Revision History:

Revision	Date	Description of changes	Requested By
0	3/2/05	Initial Release	
1	5/26/06	I.S. Manager Review	
2	10/26/06	I.S. Manager Review	

MIS108 SYSTEM
TROUBLE REPORT WORKSHEET

A. USER IDENTIFICATION:

Name: _____ Dept: _____

Phone: _____ Location _____

B. SYSTEM IDENTIFICATION

NEMHS Number: _____

Property ID: _____

C. PROBLEM DESCRIPTION

Date of Report: _____ Date problem first noted: _____

Type of Problem: (Check One) Hardware: _____ Software: _____ Not sure: _____

D. LIST COMPONENTS AND SOFTWARE AFFECTED:

E. DESCRIPTION OF PROBLEM:

F. ACTION TAKEN: For I.S. Management use only:

Date received: _____ Received By: _____

Authorization for repair: _____

Report on work completed: _____

CompletedBy: _____ Date completed: _____

Finance P&P: Information Systems
SOP # MIS109 Revision:REV.2
Effective Date:_____

Prepared by:_____
CFO Approval:_____
CEO Approval:_____

Title: MIS109 CONTROL OF COMPUTER SPYWARE, ADWARE AND SPAM

Policy: Sending and receiving e-mail is one of the most popular activities on the internet. These often originate through e-mail attachments or visiting internet sites.

Purpose: To define NEMHS policy regarding the compromise of sensitive data transmitted through e-mail and other computer communications. This policy further delineates actions required to erase such files on NEMHS computing assets.

Scope: This policy applies to all NEMHS personnel and computer systems.

Procedure:

1.0 RESPONSIBILITIES

- 1.1 The Information Systems Manager shall be responsible for training users on controlling spyware, adware, and spam. The Information Systems Manager shall develop procedures and train other Information Systems Department personnel. Additionally, the IS Manager shall be responsible for evaluating and updating appropriate detection software.
- 1.2 Department Managers shall coordinate actions required to prevent these types of outbreaks. When such programs are suspected or detected, the IS Manager shall coordinate all actions required to eradicate them and recover user data to the greatest extent possible.
- 1.3 Users shall follow the guidelines of this policy document. When a spyware, adware or spam programs are suspected, users shall immediately notify the IS Manager and the Department Managers using MIS 108 -Exhibit 1 System Trouble Shooting Report. Users shall not take any action to eradicate or recover from these programs.

2.0 DEFINITIONS

- 2.1 Spyware, Adware, and SPAM are script or code that run without your permission.

3.0 SYMPTOMS

- 3.1 Symptoms of these types of programs:
 - An unexpected or unwanted message on the screen
 - Unexplained increase in file sizes
 - Increase in the number of bad disk sectors
 - Major changes in system performance
 - Corruption of data files
 - Failure of applications software that previously worked correctly

- Warning by computer detection software

3.2 Users detecting any of these symptoms should immediately contact the IS Manager and notify the Department Manager for further investigation. Users shall not troubleshoot suspected virus attacks.

4.0 PREVENTION PROCEDURES

4.1 Only software specifically authorized by the Information Systems Department shall be installed on NEMHS computer systems.

4.2 Only personnel from the Information Systems Department shall be allowed to install and configure software on NEMHS systems.

4.3 Commercially available computer protection software shall be installed on all NEMHS computer systems. Only detection software approved by the International Computer Security Association (formally NCSA and now ICSA Labs a division of TruSecure Corporation) shall be selected for installation on NEMHS systems.

4.4 Users shall receive training, at least annually and when new software is introduced, on their computers, including security policy and preventing these types of programs from entering their computers. This training session shall also include indoctrination into how to operate the computer protection software installed on their system. Users shall be trained in how to scan for these types of files. Only Information Systems Department personnel shall carry out recovery procedures.

4.6 All software shall be scanned for viruses before installation.

4.7 All floppy diskettes shall be scanned before use. Detection software installed on user workstations and file servers shall be configured to scan floppy disks before accessing data from these drives.

5.0 ERADICATION

5.1 All NEMHS computing assets shall have an ICSA approved detection software program installed at all times. Each of these programs must be updated routinely. The Information Systems Staff shall ensure that the most up to date version of this software is available for users. Each of these off-the-shelf programs has unique procedures for handling outbreaks when detected. The Information Systems Staff shall follow the recommended procedures of the off-the-shelf program in use by the user.

5.2 IS Department personnel will perform sanitation of infected equipment and complete the Information Systems Equipment Sanitization Record (MIS 109 Exhibit 2). A Equipment Relocation Control Log (MIS 109 Exhibit 1) will also be maintained when equipment is moved.

Revision History:

Revision	Date	Description of changes	Requested By
0	3/2/05	Initial Release	
1	5/26/06	I.S. Manager Review	
2	10/26/06	Change Font	

MIS 109 EXHIBIT 2 NEMHS INFORMATION SYSTEMS EQUIPMENT SANITIZATION RECORD

Equipment & Requestor Information:

Date Requested: _____ Department or Location: _____

Person Submitting Request: _____

Equipment Serial Number: _____

Equipment Inventory Number: _____

Equipment Manufacturer/Model: _____

Equipment/Media Type: _____

Workstation User Name: _____

Magnetic Disk (Bernoulli, floppy, hard disk, removable rigid disk): _____

CDROM (read many-write many, read only, write once-ready many (WORM): _____

Memory (DRAM, PROM, EAPROM, EPROM, FEPRM, ROM, SRAM etc.): _____

Monitor: _____

Printer: _____

Other (describe):

Disposition : Transfer ____ Surplus _____ Donation _____ Repair/maintenance

Return to Contractor Other (explain) _____

Decommissioning provisions:

Equipment/media has been kept in continuous physical protection until sanitization. _____

Temporary backups made (e.g., for equipment scheduled for repair). _____

OEM operating system and other software available for reload for repurposed equipment. _____

Fixed Asset or Minor Equipment documents completed. _____

Organization asset management procedures completed. _____

Compliant with procedures for disposal of hazardous waste if destroyed. _____

Other (describe): _____

General description of data residing on equipment/media to be sanitized: _____

Person Performing Sanitization:

Title: _____ Date Completed: _____

Signature: _____

Sanitization Method Used:

DoD-compliant Overwrite (list software used):

Type I Degausser

Type II Degausser II

Chip Erase

Ultraviolet Erase

Physical Destruction (disintegrate, incinerate, pulverize, shred, and melt)

Other (describe) _____