

ITS Security Procedure: End User Device UNMC Information Technology Services

Introduction

UNMC business is conducted with [end user devices](#) (i.e. including but not limited to workstations, PCs, Macintoshes, UNIX workstations, and other desktop machines dedicated to a single user's activity) as well as mobile devices such as PDAs, laptops, printers, etc. Protection of these devices and the [information](#) handled by these systems is an essential part of doing business at UNMC. To this end, this policy provides [information security](#) instructions applicable to the [workforce](#) who use [end user devices](#) at UNMC. This policy applies to all workstation or mobile devices whether the devices are stand-alone, or connected to the campus network or the Intranet.

Note: End user devices which connect to the network from off campus must comply with the Remote Access Policy.

Basis For Policy

UNMC strives to maintain access for its faculty, staff, students, administrators and Regents (the “users”) to automated systems in accordance with [Executive Memorandum 16](#), Responsible Use of University Computers and Information Systems.

Policy

A. Configuration Control

Appropriate Software

Users are allowed to use any software packages that they feel will help them accomplish business or academic goals. Do not install or use any software unless the user explicitly trusts the source. Users must be wary of downloaded software due to the inherent risk.

There are some classifications of software that are expressly forbidden because of security reasons. Generally, users are not allowed to use software that intercepts data that they are not intended to see, interrupts the

flow of data, modifies data they do not have permission to modify, jeopardizes the integrity of the information technology resources, or fabricates any [information](#). If any of the following software is needed, please contact ITS Help Desk at 559-7700 or your designated support person.

Spyware

Spyware is software that is used to gather sensitive [information](#) or to test for weaknesses in systems. Examples of spyware include packet sniffers, port scanners, password cracking tools, and vulnerability testers.

Malicious Code

Malicious code refers to software that when run by an unsuspecting user, performs some unintended (and often unseen) task. Examples of malicious code include viruses, worms, Trojan horses, backdoors, and covert channels.

Peer-to-Peer file sharing

Peer-to-Peer file sharing software is used to share files with users over the Internet bypassing the firewall security. Examples of Peer-to-Peer software include Morpheus, Napster, Kazaa, Gnutella, Gokster, Aimster, and Imesh. These tools are mainly used to distribute copyright material illegally.

Security Bypass

Security bypass software is software that is used to circumvent security mechanisms. Examples of security bypass software are “GoToMyPC”, and dsniff.

Remote Control (modem attached to workstation)

Remote control software is software that is used to remotely control or administer a system from another system. Examples of remote control software are Terminal services, PC Anywhere, and Back Orifice.

Note: PCAnywhere is allowed on campus or when utilized through the [VPN](#).

Network Management

Network management software is software that is used to gather [information](#) from and to control network equipment. Only the UNMC Technical Services is allowed to use network management software on network equipment.

UNMC ITS will periodically scan the network to look for signs of the above mentioned software. These scans are done to ensure the integrity of the network. If the above mentioned software is found, the user will be contacted to obtain compliance to the policy. If you have questions about the use or classification of a particular software package, please contact UNMC ITS Helpdesk at 559-7700.

Users should not utilize a program to scan the network or any other device for which they are not directly responsible.

B. Access Control

Access Control: It is the responsibility of the [workforce](#) to ensure that the workstation is accessed only by authorized individuals. A member of the [workforce](#) should not utilize a device which they are not authorized to use. In addition, each member of the [workforce](#) should ensure that the devices for which they are responsible are secure according to the guidelines in this procedure.

[Confidential Information](#) on Mobile devices (such as PDA's laptops): Members of the [workforce](#) must utilize password protection. All computerized [confidential information](#) should be encrypted where technically feasible. The use of physical security measures such as using safes, locking furniture drawers, and locking office doors is recommended as a supplementary measure to protect [confidential information](#). Members of the [workforce](#) are responsible for ensuring information obtained and stored on mobile devices is obtained pursuant to the [UNMC Policy No. 6051, Computer Use and Electronic Information Security](#).

C. Viruses

Virus Protection Program Installed: All devices must run a virus detection package, if available, ITS recommends the university-wide approved software which can be downloaded from the <http://info.unmc.edu> under the quick link called "software updates". All other antivirus software must be approved by UNMC ITS prior to use to ensure they provide adequate protection. This package must run when the device is turned on. Virus detection software must be installed to automatically update weekly.

Removing Viruses: If [workforce](#) members suspect a device has been compromised or infected by a virus, they must immediately stop using the involved device and immediately call the ITS Helpdesk at 559-7700 or designated support person.

D. Back-Up

Licenses: Software license documentation must be retained to get technical support, qualify for upgrade discounts, and verify the legal validity of the licenses.

Copyright Protection: UNMC strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Making unauthorized copies of licensed and copyrighted software, even if only for "evaluation" purposes, is strictly forbidden. (See [UNMC Policy No. 6036, Reproduction of Copyrighted Materials](#))

Periodic Back-Up: All [information](#) resident on UNMC/NHS/UMA/UDA computer devices must be periodically backed-up. [Workforce](#) members are highly encouraged to store their data on network file servers. ITS ensures that network file servers are backed up according to policy (See UNMC ITS Security Procedure: Business Continuity Plan).

Data stored on local devices (i.e. local hard drives, CD's, diskettes, etc). If a member of the [workforce](#) chooses to store data on a local device, the member of the [workforce](#) is responsible for ensuring there is a backup copy. All backups should be clearly labeled (marked) with an appropriate label.

E. Destruction

Deletion of Old Information: Workers are required to delete information from their devices if it is clearly no longer needed or potentially useful. Prior to deleting any UNMC information, workers should consult the [Record Retention Schedule](#).

Destruction of Information: Media (i.e. paper, diskettes, CD's, etc) containing [confidential information](#) must be disposed of in recycle bins or via a shredder. (see UNMC Policy No. 6056, Retention and Destruction/Disposal of Private and Confidential Information)

Disposal of Equipment. All equipment must be disposed of in a manner to ensure that all information is removed. (See UNMC ITS Security Procedure: Hardware In/Out of Campus)

G. Communication

Modems: Incoming internal or external modems in network connected user devices must not be enabled. Enabled outgoing internal or external modems in network connected devices must be registered with UNMC ITS. Mobile and telecommuting devices are an exception to this rule. Remote users needing to make connections with computers must route their connections through ITS managed modems or the [Virtual Private Network](#) (VPN).

Establishing Networks: Members of the [workforce](#) must not establish local area networks, modem connections to existing internal networks, or other multi-user systems for communicating [information](#) without consulting with ITS Technical Services. This policy helps ensure that all UNMC/NHS/UMA/UDA networked systems have the controls needed to prevent unauthorized access.

IP Address: Users must not assign their own IP address to a device. An IP address must be obtained from the ITS network coordinator or the device must be configured to utilize [DHCP](#).

H. Physical Security

Equipment: If equipment has been vandalized, lost, stolen, or is otherwise unavailable for normal business activities, a [workforce](#) member must promptly inform the involved department manager and [Campus Security](#) at 559-5111. Device equipment must not be moved or relocated without the knowledge and approval of the designated support person. The designated support person must inform ITS of the change in order to maintain documentation of the network.

Placement of Display Screens: The display screens for all devices used to handle [confidential data](#) must be positioned or shielded such that the information cannot be readily viewed by non workforce members.

Printing: [Confidential](#) printed material must not be left on unattended printers.

Locking Sensitive Information: When not being used by authorized [workforce](#) members, all removable computer storage media (floppy disks, tapes, CD-ROMs, etc.) containing [confidential information](#) must be locked in secure enclosures (i.e. locked file cabinet, locked furniture drawers etc).

Environmental Considerations: Those devices with critical production applications should have emergency power where possible.

I. Management

Rights to Programs Developed: Ownership of all programs and documentation generated by, or provided by workers for the benefit of UNMC is determined by the [Ownership of Intellectual Property](#) (RP-4.4.1)

Reporting Problems: Users must promptly report all suspected unauthorized access or tampering with the [end user device](#) to the Helpdesk or designated support person.(See UNMC ITS Security Procedure: Incident Security Reporting and Response Policy).

Definitions

End User Device is a device used by a member of the [workforce](#) to accomplish access to the [information technology resources](#). Examples would include PC's, laptops, printers, PDA's and other devices.

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses on an organization's network.

Information is data presented in readily comprehensible form. (Whether a specific message is informative or not depends in part on the subjective perceptions of the person who receives it.) Information may be stored or transmitted via electronic, media on paper or other tangible media, or be known by individuals or groups.

Information technology resources (system) include but are not limited to voice, video, data and network facilities and services.

Privacy is defined as the right of individuals to keep information about themselves from being disclosed.

Confidential information means [proprietary information](#) and [protected health information](#).

Proprietary information refers to [information](#) regarding business practices, including but not limited to, financial statements, contracts, business plans, research data, [employee records](#) and [student records](#).

(a) *Employee records* refers to all information, records and documents pertaining to any person who is an applicant or nominee for any University personnel position described in the [Board of Regents Bylaws, § 3.1](#), regardless of whether any such person is ever actually employed by the University, and all information, records and documents pertaining to any person employed by the University.

(b) *Student records* refers to all information and documents of academic, demographic, or financial data pertaining to one student or to many students in a single record, on lists, or in aggregated data format.

(NOTE: the [HIPAA privacy](#) regulation does not apply to education records covered by [FERPA](#).)

Protected Health Information (PHI) is individually identifiable health information. Health information means any information, whether oral or recorded in any medium, that:

- a) . is created or received by UNMC; and
- b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

- c) *Designated* record set is the medical and billing record. Records containing PHI, in any form, are the property of UNMC. The PHI contained in the record is the property of the individual who is the subject of the record.

Information security is defined as the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss.

Workforce refers to faculty, staff, volunteers, trainees, students, independent contractors and other persons whose conduct, in the performance of work for UNMC, is under the direct control of UNMC, whether or not they are paid by UNMC.

Virtual Private Network (VPN) A Virtual Private Network refers to an encrypted communication link between the campus network and the public Internet. Since all data passing through the communication link is encrypted, it is referred to as being virtually private.

For more information, contact the ITS Helpdesk.

[ITS HIPAA Policies Home Page / Top of this Page](#)

This is a new policy.

This page updated on , by .