COMPUTER USE AND ELECTRONIC INFORMATION SECURITY POLICY

Introduction

UNMC has a robust information technology environment. It is the responsibility of the workforce to utilize information technology resources in an appropriate manner. Individuals with access to information systems are expected to safeguard resources and maintain appropriate levels of confidentiality.

Basis for Policy

The University of Nebraska has issued Executive Memorandum No. 16, Policy for Responsible Use of Information Resources (https://nebraska.edu/offices-policies/policies/no-16-policy-for-responsible-use-of-university-computers-and-information-systems/#Web), which sets forth the University's administrative policy and provides guidance relating to the responsible use of the University's electronic information systems. It is the intent of this policy to confirm campus adherence to Executive Memorandum 16.

Information technology resources are owned by UNMC and are intended for use in completing UNMC's mission. Their use is governed by Executive Memorandum No. 16, all applicable UNMC policies (https://wiki.unmc.edu/index.php/Policies_and_Procedures/), including sexual harassment, patent and copyright, patient and student confidentiality, and student and employee disciplinary policies, as well as by applicable federal, state and local laws.

Policy

Acceptance and Adherence to Policy

Using UNMC's information systems by anyone shall constitute agreement to abide by and be bound by the following:

1. Provisions of this policy
2. UNMC Information Security Procedures (https://info.unmc.edu/its-security/policies/procedures/)
3. UNMC Policy 6045, Privacy, Confidentiality and Information Security (https://wiki.unmc.edu/index.php/Privacy/Confidentiality/)
4. Executive Memorandum No. 16, Policy for Responsible Use of Information Resources (https://nebraska.edu/offices-policies/policies/no-16-policy-for-responsible-use-of-university-computers-and-information-systems/#Web)
5. Executive Memorandum No. 26, University of Nebraska Information Security Plan (https://nebraska.edu/offices-policies/policies/no-26-university-of-nebraska-information-security-plan----gramm-leach-bliley-compliance/#Web)
6. Executive Memorandum No. 27, HIPAA Compliance Policy (https://nebraska.edu/offices-policies/policies/no-27-hipaa-compliance-policy/#Web)

Access

Physical and electronic access to proprietary information and computing resources is controlled. The level of control will depend on user need and the level of risk and exposure to loss or compromise. Access will be assigned based upon the information needed to perform assigned duties. On campus electronic access is controlled through user id and password. Off Campus electronic access in some instances requires two-factor authentication.

UNMC Net ID accounts

UNMC Net ID accounts will only be issued to the following individuals:

1. Faculty, staff and students of UNMC
2. Retired faculty who have an emeritus appointment
3. Individuals who have a relationship with UNMC and need access to electronic resources in order to perform their duties.
   a. Individuals must have a department chair or section chief sponsor their need for this account.
   b. The department chair or section chief is responsible for ensuring that the individual is aware of all UNMC policies and procedures relating to the use of the electronic resources.
   c. The department chair or section chief is responsible for coordinating with ITS to ensure that all software license regulations are honored by granting this account.
   d. ITS is responsible for maintaining a log of
      i. Individual name
      ii. Contact information
      iii. Sponsoring Department Chair or Section Chief
      iv. Resources accessed
      v. Reason for account/relationship to UNMC
   e. The Assistant Vice Chancellor or designee will approve requests for these types of accounts.

UNMC email accounts

UNMC email accounts will only be issued to the following individuals:

1. Faculty (excluding volunteer appointments) staff and students of UNMC
   a. Upon an employee's entry into SAP or a student being admitted to a program, an email account will automatically be generated. It is the expectation that all faculty/staff/students will read and maintain their UNMC email account. Important information regarding the activities of UNMC is communicated via email.
2. Retired faculty who have an emeritus appointment
3. If a department identifies the need for an individual who does not meet the criteria to have an email account, a request for a policy exception can be made:
   a. Individuals must have a department chair or section chief sponsor their need for this account.
   b. The department chair or section chief is responsible for ensuring that the individual is aware of all UNMC policies and procedures relating to the use of the electronic resources.
   c. The department chair or section chief is responsible for coordinating with ITS to ensure that all software license regulations are honored by granting this account.
   d. ITS is responsible for maintaining a log of
      i. Individual name
      ii. Contact information
      iii. Sponsoring Department Chair or Section Chief

iv. Resources accessed
v. Reason for account/relationship to UNMC

e. The Assistant Vice Chancellor or designee will approve requests for these types of accounts.

NOTE: If an individual is a volunteer, please refer to UNMC Policy No. 6053, Volunteer (https://wiki.unmc.edu/index.php/Volunteer/).

Individual Personal accounts will always be utilized to access confidential information.

Users are responsible and accountable for access under their personal accounts. No one should use the ID or password of another, nor should anyone provide his or her ID or password to another, except in the cases necessary to facilitate computer maintenance and repairs. Your password should only be given to Information Technology Support Personnel upon presentation of identification. If your password is shared with Information Technology Support Personnel, where technically feasible the password should be flagged, necessitating that it be changed the next time the user logs on.

A strong password is the "first defense" against an information security attack upon the UNMC network. It is imperative that all users select a strong password. (See ITS Security Procedure: Password Security (https://info.unmc.edu/its-security/policies/procedures/passwords.html)).

Access to electronic mail, voice mail, administrative, student and patient care information systems will be obtained through the appropriate authorization process. (See ITS Security Procedure: Access Control to IT Resources (https://info.unmc.edu/its-security/policies/procedures/access-control.html)). Unauthorized access to information systems is prohibited. Users must not attempt to gain access to information or systems for which they are not granted access.

Remote access to systems which contain confidential information will be accomplished through a strong authentication method with the appropriate approval processes. Individuals requiring remote access to UNMC's email system will purchase an internet service provider and utilize the web based email product.

Information Technology Support Personnel will inactivate or delete IDs/password, as appropriate, of individuals who no longer have a relationship with UNMC.

Appropriate Use

It is the responsibility of the workforce to utilize the information technology resources in an appropriate manner. Individuals with access to information systems are expected to safeguard resources and maintain appropriate levels of confidentiality in order to protect the integrity of all data and of the interests of the entity.

It is the responsibility of the workforce to protect confidential information at all times including, but not limited to, when stored electronically (at rest) and when the data is being transferred outside of the facility such as on a mobile device or a diskette (See ITS Security Procedure: End User Device (https://info.unmc.edu/its-security/policies/procedures/enduser.html)).

UNMC's information technology resources are to be used predominately for completing UNMC work related business. Misuse of University information systems is prohibited. Misuse includes the following (see Executive Memorandum No. 16, Policy for Responsible Use of Information Resources (https://nebraska.edu/offices-policies/policies/no-16-policy-for-responsible-use-of-university-computers-and-information-systems/#Web))

1. Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.
2. Accessing without proper authorization computers, software, information or networks which the University belongs, regardless of whether the resource accessed is owned by the University or the abuse takes place from a non-University site.
3. Taking actions, without authorization, which interfere with the access of others to information systems.
4. Circumventing logon or other security measures.
5. Using information systems for any illegal or unauthorized purpose.
6. Personal use of information systems or electronic communications for non-University consulting, business or employment, except as expressly authorized pursuant to Section 3.4.5 of the Bylaws of the Board of Regents.
7. Sending any fraudulent electronic communication.
8. Violating any software license or copyright, including copying or redistributing copyrighted software, without the written authorization of the software owner.
9. Using electronic communications to violate the property rights of authors and copyright owners. (Be especially aware of potential copyright infringement through the use of e-mail.)
10. Using electronic communications to harass or threaten users in such a way as to create an atmosphere which unreasonably interferes with the education or the employment experience. Similarly, electronic communications shall not be used to harass or threaten other information recipients, in addition to University users.
11. Using electronic communications to disclose proprietary information without the explicit permission of the owner.
12. Reading other user's information or files without permission.
13. Academic dishonesty.
14. Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records (including computerized records, permits, identification cards, or other documents or property).
15. Using electronic communications to hoard, damage, interfere with academic resources available electronically.
16. Using electronic communications to steal another individual's works, or otherwise misrepresent one's own work.
17. Using electronic communications to fabricate research data.
18. Launching a computer worm, computer virus or other rogue program.
19. Downloading or posting illegal, proprietary or damaging material to a University computer.
20. Transporting illegal, proprietary or damaging material across a University network.
21. Personal use of any University information system to access, download, print, store, forward, transmit or distribute obscene material.
22. Violating any state or federal law or regulations in connection with use of any information system.

Persons using UNMC's information technology facilities and services bear the primary responsibility for the material they choose to access, send or display. It is a violation to access and view materials which would create the existence of a sexually hostile working, patient care, or educational environment.

It is the workforce's responsibility to notify ITS when an information security incident appears to have happened. (See ITS Security Procedure: Information Security Incident Reporting and Response (https://info.unmc.edu/its-security/policies/procedures/incident-reporting.html)). A security incident includes, but is not limited to the following events, regardless of platform or computer environment:

1. Evidence of tampering with data
2. System is overloaded to the point that no activity can be performed (Denial of service attack on the network)
3. Web site defacement
4. Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources)
5. Social engineering incidents
6. Virus attacks which adversely affect servers or multiple workstations
7. E-mail which includes obscene material, threats or material that could be considered harassment
8. Discovery of unauthorized or missing hardware in your area
9. Other incidents that could undermine confidence and trust in the UNMC's information technology systems

ITS or other personnel must take immediate action to mitigate any threats that have the potential to pose a serious risk to campus information system resources. If the threat is deemed serious enough, the system(s) or individual posing the threat will be blocked from network access. Communication with department leadership regarding such action will take place as soon as possible. The block will be removed as soon as the threat has been repaired.

Copyright

UNMC maintains strict compliance with the Digital Millennium Copyright Act of 1998 and applicable amendments. It should be noted that traditionally a user purchases a software "license," which is a right to use. Many times the licenses can only be loaded on one machine. Violating any software license or copyright is in violation of university policy.

1. Executive Memorandum No. 16, Policy for Responsible Use of Information Resources (https://nebraska.edu/offices-policies/policies/no-16-policy-for-responsible-use-of-university-computers-and-information-systems/#Web)
2. The Digital Millennium Copyright Act of 1998 (http://www.copyright.gov/legislation/dmca.pdf)
3. U.S. Copyright Office - General Guidelines About Copyright Law (http://www.copyright.gov/)
4. UNMC Policy No. 6036, Reproduction of Copyrighted Materials (https://wiki.unmc.edu/index.php/Reproducing_Copyrighted_Materials/)
5. Public Affairs Copyright and Disclaimer

Privacy

Users should be aware that privacy cannot be guaranteed. UNMC ITS staff do not regularly audit e-mail, voice mail or other information systems for content except under the direction of UNMC internal investigations. However, users should be aware that UNMC information technology technical personnel have authority to access individual user files, data and voice mail in the process of performing repair, maintenance of information systems or supporting UNMC internal or external investigations (See UNMC Policy No. 6055, Fraud (https://wiki.unmc.edu/index.php/Fraud/) and Executive Memorandum No. 16, Policy for Responsible Use of Information Resources (https://nebraska.edu/offices-policies/policies/no-16-policy-for-responsible-use-of-university-computers-and-information-systems/#Web)). In the event violations to this policy are discovered as a result of the maintenance activity, ITS will bring the issue to the attention of the appropriate dean, director or department head and the Assistant Vice Chancellor for Human Resources.

UNMC Information Technology Services will not release IDs/passwords for voice mail or information systems to anyone other than the user without explicit review by and permission from the Assistant Vice Chancellor for Human Resources or Vice President General Counsel.

E-mail, Instant Messaging and Voice Mail

All policies stated herein are also applicable to all communication systems including e mail, instant messaging and voice mail. Persons using UNMC's e mail or voice mail resources are expected to demonstrate good taste and sensitivity to others in their communications.

E-mail attachments and files transfer utilizing instant messaging capabilities represent a significant risk to the organization. Many computer viruses are distributed through e-mail attachments or files received via instant messaging. Users should be careful about opening e-mail attachments or accepting file transfers via instant messaging.

Controlling the Distribution of Non-Solicited Marketing E-mail

Electronic mail sent externally by UNMC personnel for the primary purpose of promoting UNMC's "commercial" products or services must comply with the ITS Security Procedure: Controlling the Distribution of Non-Solicited Marketing Email (https://info.unmc.edu/its-security/policies/procedures/spam-compliants.html). Examples of such products or services include publications and membership solicitations.

The Act is applicable only to e-mail that constitutes a commercial advertisement or promotion of a commercial product or service. The Act is not applicable to commercial e-mail in general, to e-mail advertising or promoting "activity" or to e-mail simply because the e-mail references or solicits funds. Further, it is not applicable to e-mail messages sent to provide information about UNMC's undergraduate, graduate, or professional degree-granting programs. Some programs not a part of the regular campus curriculum might be considered commercial "services" depending upon the facts. Advice from the Compliance Officer should be sought about such programs.

Exemptions

The Act exempts "transactional or relationships messages" from the procedural requirements when the primary purpose of the message is to achieve one of the following:

- Facilitate, complete or confirm a commercial transaction that the recipient has previously agreed to, such as messages confirming registration, purchase or reservations.
- Provide warranty information or product recall or safety/security information with respect to a product or service used or purchased by the recipient.
- Notify the recipient about substantive changes in an existing subscription or related benefit plan in which the recipient is currently participating.
- Deliver goods or services, including upgrades or updates, which the recipient has previously requested or ordered from the sender.

For more information, see ITS Security Procedure: Controlling the Distribution of Non-Solicited Marketing Email (https://info.unmc.edu/its-security/policies/procedures/spam-compliants.html).

Campus-wide e-mail announcements

Sending out mass distribution e-mails containing event and/or general announcement type information is discouraged. If you have an event to publicize or an announcement to deliver to a large group of people, the best way to do this is through UNMC Today, the campus electronic newsletter. Contact Public Relations for additional information.

However, if e-mailing to a large group is warranted, the content and size of the message must be approved by Public Relations. Delivery of the message must then be scheduled by the ITS department to minimize the demand on campus computer systems. Contact Public Relations (x9-4696) to obtain approval.

Audits of Electronic Protected Health Information (PHI)

Patient information including demographic and medical data contained in, or obtained from any UNMC information system is confidential data. Individual access to this data may be audited in order to ensure compliance with federal and state law and UNMC Policies and Procedures (https://wiki.unmc.edu/index.php/Policies_and_Procedures/).

Information Systems

Each information custodian is responsible to:

1. Manage and approve access to the information.
2. Implement audit mechanisms.
3. Develop periodic audit process to validate that only those with a need to know are accessing ePHI (See UNMC Policy No. 6057, Use and Disclosure of Protected Health Information (https://wiki.unmc.edu/index.php/Protected_Health_Information_(PHI/)).
4. Develop and implement a formal process for audit log review.
5. Audit reports are confidential and should not be released without the approval of the HIPAA debrbishop@nebraskamed.com or the Human Resources Employee Relations Manager.

Shared Files

The owner of shared files is responsible to:

1. Manage and approve access to the information
2. Implement process such that the minimum necessary information is available to the user (See UNMC Policy No. 6057, Use and Disclosure of Protected Health Information (https://wiki.unmc.edu/index.php/Protected_Health_Information_(PHI/)).

Computer Crime

Computer crime in any form will not be tolerated. This policy applies to all UNMC employees and will be enforced without regard to past performance, position held or length of service. All persons found to have committed computer crime relevant to UNMC assets shall be subject to disciplinary action up to and including termination and investigation by external law enforcement agencies when warranted.

Security Administration

UNMC ITS is responsible for implementing and monitoring a consistent data security program. System administrators are responsible for operation and maintenance of information processing services. The system administrator and information custodians are responsible for implementing the security policy and standards within their applications.

Training

All members of the workforce will be trained in information security awareness. Periodic reminders regarding information security awareness and current threats will be communicated to the workforce.

Web Pages

UNMC web pages should consistently meet the highest standards of writing, content accuracy, image and presentation, keeping in mind that these documents create an image of UNMC to the world. UNMC shall reserve the right to monitor web pages and to remove any material that is unlawful or in violation of UNMC policies. Originators will be notified in the event that their page is removed.

UNMC procedures and guidelines for web page development should be observed. The web handbook is also a useful tool. These guidelines are not intended nor do they supersede in anyway the well-recognized rights of academic freedom. UNMC web pages are required to show:

1. Date of the last revision
2. Hot e-mail link to person responsible for the page
3. UNMC logo (per Executive Memorandum 16)
4. Link back to appropriate UNMC site (Internet or Intranet)
5. Link to University of Nebraska Appropriate Use/Copyright Violations

Faxing

Members of the workforce will have a need to transmit confidential information by facsimile rather than by a slower method, such as mail. It is easy to misdirect faxes to unauthorized recipients, faxes could be intercepted or lost in transmission. Thus, the potential for breach of confidentiality exists every time someone utilizes faxing. Therefore, all faxing must be done in accordance with the faxing policy (See UNMC Policy No. 6065, Facsimile Transmissions (https://wiki.unmc.edu/index.php/Fax_Transmissions/)).

Demonstration of Electronic Systems

Demonstrations of electronic systems for non-workforce members should utilize only test data. Test data in production systems is acceptable. Production data (real patient data) should not be used.

Definitions

Computer crime examples would include:

1. Unauthorized use of a computer, which might involve stealing a username and password, or might involve accessing the victim's computer via the Internet through a backdoor operated by a Trojan Horse program.
2. Creating or releasing a malicious computer program (e.g., computer virus, worm, Trojan horse).
3. Harassment and stalking in cyberspace.
4. Using computers to commit crimes that could be committed without a computer such as counterfeiting, stealing, committing larceny or fraud.

(Source: Computer Crime by Ronald B. Stander, Copyright 1999, 2002, www.rbs2.com (http://www.rbs2.com/))

Confidential information includes proprietary information and protected health information (PHI).

Denial of service is an event in which a user or organization is deprived of resource services that they would normally expect to have.

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 generated in the course of University operations is a valuable asset of the University and property of the University.

Information custodians are people responsible for specifying the security properties associated with the information systems their organization possesses. This includes the categories of information that users are allowed to read and update. The information custodian is also responsible for classifying data and participating in ensuring the technical and procedural mechanisms implemented are sufficient to secure the data based upon a risk analysis that considers the probability of compromise and its potential business impact.

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.

Information systems are an interconnected set of informational resources under the same direct management control that shares common functionality.

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

Information Technology Support Personnel are the individuals who as a function of their job provide IT support. This includes ITS support staff, departmental system administrators and IT support staff within the units.

Personal accounts allow an individual user to logon to specific applications or systems using personal or unique ID and password.

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

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. (See UNMC Policy No. 6045, Privacy, Confidentiality and Information Security (https://wiki.unmc.edu/index.php/Privacy/Confidentiality/) for more detailed information.)

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

1. is created or received by UNMC; and
2. 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.

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.

Shared accounts (i.e., generic or general accounts) allow multiple users to logon to the information technology resources using the same ID and password.

Shared file is a collection of electronic PHI maintain on personal or departmental computers. This would include spreadsheets, databases, correspondence, quality improvement and research data files.

Social engineering describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

Strong authentication method is a layer of security which requires a token or biometric authentication. This represents two factor authentication involving something you know (i.e. user id) and something you have (i.e., Secured card).

System administrators are the people responsible for configuring, administering, and maintaining hardware and operating systems.

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.

Reference: University of CA Guidelines (http://www.ucop.edu/information-technology-services/), January 28, 2004

Additional information

- Executive Memorandum No. 16, Policy for Responsible Use of Information Resources (https://nebraska.edu/offices-policies/policies/no-16-policy-for-responsible-use-of-university-computers-and-information-systems/#Web)
- Executive Memorandum No. 26, University of Nebraska Information Security Plan (https://nebraska.edu/offices-policies/policies/no-26-university-of-nebraska-information-security-plan----gramm-leach-bliley-compliance/#Web)
- Executive Memorandum No. 27, HIPAA Compliance Policy (https://nebraska.edu/offices-policies/policies/no-27-hipaa-compliance-policy/#Web)
- UNMC Policy No. 6036, Reproduction of Copyrighted Materials (https://wiki.unmc.edu/index.php/Reproducing_Copyrighted_Materials/)
- UNMC Policy No. 6045, Privacy, Confidentiality and Information Security (https://wiki.unmc.edu/index.php/Privacy/Confidentiality/)
- UNMC Policy No. 6053, Volunteer (https://wiki.unmc.edu/index.php/Volunteer/)
- UNMC Policy No. 6055, Fraud (https://wiki.unmc.edu/index.php/Fraud/)
- UNMC Policy No. 6057, Use and Disclosure of Protected Health Information (https://wiki.unmc.edu/index.php/Protected_Health_Information_(PHI/)
- UNMC Policy No. 6065, Facsimile Transmissions (https://wiki.unmc.edu/index.php/Fax_Transmissions/)
- UNMC Information Security Procedures (https://info.unmc.edu/its-security/policies/procedures/)

- The Digital Millennium Copyright Act of 1998 (http://www.copyright.gov/legislation/dmca.pdf)
- U.S. Copyright Office - General Guidelines About Copyright Law (http://www.copyright.gov/)

Policy No.:	6051
Effective Date:	04/25/2007
Revised Date:	08/20/2013
Reviewed Date:	09/19/2017