Policy Title

University of Nebraska at Omaha Privacy Policy

Policy Information

- Date issued: November, 2008
- Approved by: Chancellor's Cabinet
- Last revision: November, 2008

Reason for Policy

The University of Nebraska at Omaha (UNO) values individual's privacy rights and understands the importance of these rights when storing or transmitting personal information provided by you or collected while using UNO's information systems. UNO protects the privacy of individuals and the confidentiality of official information stored on its information systems. Privacy and confidentiality, however, must be balanced with the need for the university to manage and maintain healthy and secure information systems.

University of Nebraska Executive Memorandum 16 states the expectation of privacy an individual has when utilizing University of Nebraska network and computer resources. This policy outlines UNO's approach toward enforcing the expectation of privacy set forth by Executive Memorandum 16.

Definitions

Information systems: shall mean and include computers, networks, applications, servers and other similar devices that are administered, leased, or owned by the University and for which the University is responsible.

Personal information: is information that can be associated with a specific person and can be used to identify that person. We do not consider personal information to include information that has been made anonymous. *Restricted and Sensitive Data* as defined in the *Restricted Data Security Policy* is considered personal information.

Restricted Data: is University data that is highly confidential and is covered by state or federal privacy law. Unauthorized access to restricted data could result in grievous economic or social harm to individuals and loss of the public's confidence in the University's ability to protect private information. Specific examples of restricted data are:

- Social Security Numbers
- Motor vehicle operator's license number or state identification card number
- Account or credit or debit card numbers, in combination with any required security code, or password that would permit access to a person's financial account.
- Unique electronic identification number, username or routing code, in combination with any required security code, access code or password.
- Unique biometric data, such as fingerprint, voice print, or retina or iris image, or other unique physical representation.

Responsibilities

- ***Chief Information Security Officer (CISO):*** Responsible for execution of this policy and coordinating policy enforcement with the FERPA Compliance Officer.

- **Family Education Rights and Privacy Act** (***FERPA) Compliance Officer:*** Responsible for ensuring FERPA compliance.

Entities Affected By This Policy

All members of the University community.

Who Should Read This Policy

All members of the University community.

Website Address For This Policy

http://www.unomaha.edu/policies

Related Resources

Resource	Description
http://www.nebraska.edu/about/exec_memo16.pdf	NU Executive Memorandum 16
http://www.nebraska.edu/about/exec_memo26.pdf	NU Executive Memorandum 26
http://its.unomaha.edu/cybersecurity/pdf/rdauthform.pdf	Restricted Data Authorization form
http://www.ses.unomaha.edu/registrar/ferpa.php	UNO student records policy
http://www.unomaha.edu/policies	UNO privacy policy
http://uniweb.legislature.ne.gov/FloorDocs/99/PDF/Slip/LB876.pdf	Consumer Notification of Data Security Breach Act of 2006
https://www.pcisecuritystandards.org/	Payment Card Industry Data Security Standards (PCI DSS)

Policy Overview

Personal Information

This policy describes the privacy laws UNO follows and the way UNO collects and shares your personal information. For additional information regarding security procedures of *Restricted Data*, please refer to the UNO Restricted Data Policy in the Resource Section.

University, State and Federal Privacy Laws

The following are privacy laws which UNO is required to follow:

Student records: Student records are protected by the Federal Family Education Rights and Privacy Act (FERPA), and University of Nebraska Board of Regents bylaw 5.6. These student record policies prohibit the release of students educational records, with the exception of those defined as "directory information." FERPA also states how student records are to be kept confidential. For more information on these policies, please visit:

UNO Student Records Policy: http://www.ses.unomaha.edu/registrar/ferpa.php
NU Board of Regents bylaw 5.6: http://www.nebraska.edu/board/board_bylaws.shtml

Employee records: Employee records are protected by the University of Nebraska Board of Regent bylaw 1.4.4. It specifies employee information that is to be kept confidential.

NU Board of Regents bylaw 1.4.4: http://www.nebraska.edu/board/board_bylaws.shtml

Public records law: Under the State of Nebraska Public Records Law (§§ 84-712 THROUGH 84-712.09), UNO may be required to provide information to a third party. Information protected by FERPA or by other laws or Board of Regents policy will not be disclosed in response to a public records request.

Public Records Law: http://www.ago.state.ne.us/content/records_statutes.html

Information UNO Collects About You

Academic and Administrative Information: It is UNO's policy to collect only the personally identifiable information that is needed to provide academic and administrative services to you. When you take classes at or are hired by UNO, personal information provided by you such as your name, address, Social Security Number (SSN) and related information is collected and stored on UNO computer resources. Through the course of your association with the University, additional personal information is collected and stored.

Information Systems:

In the course of ensuring healthy and secure information systems, the University has deployed automated technology devices to do such things as monitor network traffic for performance, detect unauthorized use of *Restricted Data*, identify intrusion attempts, detect SPAM, malware and other malicious attacks that might damage University information systems. Information from these devices is used solely for maintaining a healthy and secure environment for UNO information systems. UNO does not do routine monitoring that personally identifies ones' use of UNO information systems.

UNO may access or monitor personal information stored or transported on UNO information systems under the following conditions:

1. When it is necessary, as determined by the CISO or designee(s), to protect the health and security of the University information systems;
2. If during routine maintenance there is suspicion of misconduct under University policies, or Federal or State laws or if abuse complaints (http://abuse.unomaha.edu) have been filed and
   a. ***there is no*** *emergency threat to the health and security of University Information systems*, the CISO or designee(s) will pursue authorization from Human Resources (Staff), Academic Affairs (Faculty) and the Dean or Divisional Leader to investigate if policy violations are occurring.
   b. ***there is*** *an emergency threat to the health and security of University Information systems*, the CISO or designee(s) will take responsible measures to protect the health and security of University information systems. Once the threat is under control, information concerning it will be shared with Human Resources (Staff), Academic Affairs (Faculty) and the Dean or Divisional Leader to investigate if policy violations are occurring.
3. It is necessary to comply with authorized requests from law enforcement, as stated in Executive Memorandum 16. In such cases, University Legal Counsel will be consulted.

E-mail Communications: email messages, instant messages, online chats, or the content of other online communications that reside on or pass through our e-mail systems are not read unless the messages contain unencrypted *Restricted Data.* Unencrypted *Restricted Data* is filtered to comply with the *UNO Restricted Data Policy*. Incoming and outgoing email messages are generally scanned electronically to identify and filter out likely spam and malware that could harm UNO information systems. We may retain and provide communications if we are legally required to do so.

Website: University web sites routinely collect and store information from online visitors to enhance system performance and produce reports regarding website use. Information collected includes the pages visited on the site, the date and time of the visit, the internet address (URL or IP address) of the referring site, the domain name and IP address from which the access occurred, the version of browser used, the capabilities of the browser, and search terms used on our search engines. UNO makes no attempt to personally identify individual visitors from this information and does not share it with third parties.

Sharing

Personal information is only shared with authorized members of the University who have a legitimate need to know in order to provide necessary academic and administrative services. UNO may share personal information with third parties that provide services to the University. In such cases, the third parties are bound by University, State and Federal policy to protect your privacy. Personal information is only shared with those that DO NOT provide services to UNO when required to by law.

Privacy Questions

If you have questions concerning this policy, you can contact the UNO Helpdesk at 554-HELP (4357) or unohelpdesk@mail.unomaha.edu.