UNIVERSITY OF NEBRASKA AT OMAHA

Effective: 11-01-2008
Last Revised: 08-31-2016

Responsible University Administrator:
Matt Morton, Chief Information Security Officer

Responsible University Office:
Information Security

Policy Contact:
Information Security • security@unomaha.edu

Privacy Policy

POLICY CONTENTS

Scope

This policy applies to university personnel and entities who have access to and electronically store regulated data and/or collect, store, and use personal information.

Policy Statement

This policy describes the privacy laws the University of Nebraska Omaha (UNO) follows, and the way that UNO collects and shares your personal information. For additional information regarding security procedures of regulated data, please refer to the UNO Regulated Data Policy.

University, State, and Federal Privacy Laws

The following are privacy laws which UNO is required to follow for each category of data:

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 mandates how student records are to be kept confidential. The *UNO Student Records Policy* provides additional information on FERPA.

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.

Public Records

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.

Information UNO Collects About You

Academic and Administrative Information
It is the policy of UNO to collect only the personally identifiable information (PII) that is required to provide academic and administrative services to you. When you enroll in classes 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. Throughout 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 services to monitor network traffic for performance; detect unauthorized transmission of regulated data; identify intrusion attempts; and detect spam, malware, and other malicious attacks which could 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 perform routine monitoring that personally identifies one's 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 state/federal laws, or if abuse complaints have been filed, and

- **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 (for staff), Academic Affairs (for faculty), and the dean or divisional leader to investigate if policy violations are occurring.
- **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 (for staff), Academic Affairs (for 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.

Email Communications
Email messages, instant messages, online chats, or the content of other online communications that reside on or pass through our email systems are not read unless the messages contain unencrypted regulated data. Unencrypted regulated data is filtered to comply with the UNO Regulated Data Policy, NU Executive Memorandum 26, PCI-DSS, HIPAA, and FERPA. Incoming and outgoing email messages are scanned electronically to identify and filter out likely spam and malware that could harm UNO information systems. The university may retain and provide communications if we are legally required to do so.

Website

University websites 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 website, 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 university search engines. UNO makes no attempt to personally identify individual visitors from this information and does not share the data with third parties.

Sharing
Personal information is shared only 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 policies to protect your privacy. Personal information is shared only when required by law with those that do not provide services to UNO.

Privacy
If you have questions concerning this policy, you may contact the Information Security Office at 402.554.2492 or security@unomaha.edu.

Reason for Policy

UNO values individual privacy rights and understands the importance of these rights when storing or transmitting personal information provided by you or collected while using university 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 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 NU Executive Memorandum 16.

Definitions

Information System: Includes 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: Information associated with a specific person which can be used to identify that person. Personal information does not include information that has been made anonymous. "Regulated and sensitive data" as defined in the UNO Regulated Data Policy is considered personal information.

Regulated Data: University data that is highly confidential and is regulated by state or federal privacy laws. Specific examples of regulated data include:

- 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

- Student records (except those defined by university policy as directory information under FERPA)
- 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, retina/iris image, or other unique physical representation
  Health-related data

Additional Contacts

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.

Related Information

NU Executive Memorandum 16

NU Executive Memorandum 26

UNO Student Records Policy

State of Nebraska Consumer Notification of Data Security Breach Act of 2006

Payment Card Industry Data Security Standards (PCI-DSS)

State of Nebraska Public Records Law

UNO Regulated Data Security Policy

NU Board of Regents bylaw 1.4.4

NU Board of Regents bylaw 5.6

State of Nebraska Public Records Law

History

This policy is an update to the Privacy Policy that was previously updated in 2008.
