UNIVERSITY OF NEBRASKA AT OMAHA

Effective: 10-01-2014
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

Regulated Data Security

POLICY CONTENTS

Scope

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

Policy Statement

Regulated Data Storage

All personnel and entities associated with the university that intentionally store regulated data electronically are required to seek authorization by completing the form in Appendix B: Regulated Data Authorization Form. This includes third parties that provide services to the university and those requirements mandated by law such as financial aid and payroll. Authorization to electronically store regulated data does not grant permission to share that data with anyone. Electronic storage of regulated data is not permitted on non-university owned devices unless specifically authorized. You must contact the Information Security Office for assistance in disposing any regulated data.

Risk Reduction and Enforcement

Data scanning software for data loss prevention (DLP) has been installed on the University of Nebraska Omaha (UNO)'s network to help reduce the risk of data breaches. This device is intended only to flag network traffic and data storage that contains unencrypted regulated data. The information found by the DLP software is strictly used to reduce the risk of regulated data being breached. Access to reports generated by DLP software is authorized by the Executive Regulated

Data Authorization Committee only for the use of enforcing this policy and reducing the exposure of regulated data. The use of DLP software complies with NU Executive Memorandum 16 and the UNO Privacy Policy.

Reason for Policy

Identity theft continues to rise every year in the United States. The use of the Internet to steal sensitive data such as Social Security Numbers (SSN) and payment card numbers is a major contributor to this rise.

Institutions of higher education have become attractive targets for Internet identity theft. Data credentials such as SSNs are used by thieves to establish fraudulent credit and perform other illegal activities associated with stealing a person's identity. UNO has legal and ethical responsibilities to protect this sensitive data. Failure to do so may result in economic or social harm to individuals, loss of the public's confidence in the university's ability to protect sensitive data, and legal liability for damages incurred.

The State of Nebraska approved LB 876, known as the "Consumer Notification of Data Security Breach Act of 2006," in April 2006. This law outlines what must occur if unencrypted data, as defined in the Act, has been breached. In addition, UNO must comply with Payment Card Industry (PCI) requirements to properly secure payment card information. Failure to meet these requirements may result in financial penalties and/or loss of ability to process payment cards at UNO. As stewards of personal information, UNO has a responsibility to be vigilant and proactive in the protection of privacy of campus users and the protection of regulated data that has been entrusted to its care. This policy serves to identify procedures and security requirements that must be met before authorization is granted to electronically store regulated data.

Procedures

Requesting Access to Electronically Store Regulated Data

To be granted access to electronically store regulated data, you must first complete the request form located in Appendix B: Regulated Data Authorization Form.

Once the request form is completed and signed by an Academic Dean or Divisional Leader, then the request will be considered for authorization by the Regulated Data Authorization Committee. If a regulated data storage request is denied by the Regulated Data Authorization Committee, the requester may appeal to the Executive Regulated Data Authorization Committee. The Executive Regulated Data Authorization Committee will make the final decision regarding the storage of regulated data. Reauthorization to continue to electronically store regulated data is required on a biennial basis.

Information Services (IS) provides a Regulated Data Server for any authorized individual or department to use. If the IS Regulated Data Server will not be used, the proposed storage location must meet the technical security requirements outlined in Appendix B: Regulated Data Authorization Form.

Regulated Data Storage Requirements

Technical Requirements

All regulated data must be stored on the Regulated Data Server managed by IS. Updates will continue to be made to these requirements as technology and cybersecurity threats change. Authorized users will be notified as changes are made.

Audits
All university-owned equipment is subject to audit for unauthorized storage of regulated data. Devices authorized to store regulated data are subject to audits as deemed necessary by the Information Security Office. Reasonable prior notification of an audit will be provided. Audit results are handled confidentially by Information Security staff and are reported to the Executive Regulated Data Authorization Committee in aggregate.

Training
Training on technical requirements will be provided at the time authorization is granted to electronically store regulated data by IS. Training must be completed before storage of regulated data begins.

Policy Enforcement
This policy is enforced by the Executive Regulated Data Authorization Committee. Failure to comply with this policy may result in disciplinary actions.

Definitions

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

Sensitive Data: University data routinely used in conducting business not covered by state or federal privacy laws. The data are protected to preserve the privacy, safety, and reputation of individuals and/or the university.

Public Data: University data which are categorized as neither "regulated" nor "sensitive." Generally, this is information that can be made available to the public without risk of harm to the university or any entities with an affiliation to the university.

Additional Contacts

Executive Regulated Data Authorization Committee

This committee consists of the Associate Vice Chancellor for Research and Creative Activity, Associate Vice Chancellor for Student Affairs, Chief Information Officer (CIO), and Associate Vice Chancellor for Business and Finance. The committee members are responsible for reviewing decisions of the Regulated Data Authorization Committee as requested. This committee is responsible for the enforcement of this policy.

Regulated Data Authorization Committee
This committee consists of the Director of Records and Registration, Director of Finance and Controller, and Chief Information Security Officer (CISO). These members are responsible for authorizing access to store regulated data and executing this policy.

Data Users
Data Users are individuals authorized to access and electronically store regulated data in execution of their job functions. Users are responsible for taking all reasonable measures to safeguard the confidentiality and integrity of the data to which they have access. This group includes outside parties contracted to perform data services.

Academic Deans and Divisional Leaders
Academic Deans and Divisional Leaders are responsible for coordinating with the Regulated Data Authorization Committee in authorizing their staff's request to electronically store regulated data.

Information Security Office (within Information Services)
The Information Security Office is responsible for enforcing the technology requirements outlined in this policy.

Forms

Regulated Data Security Policy Form (Appendix B)

Related Information

Regulated Data Standard

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)

History

This policy is an update to the Regulated Data Security Policy that was previously updated in 2014.

The University of Nebraska does not discriminate based on race, color, ethnicity, national origin, sex, pregnancy, sexual orientation, gender identity, religion, disability, age, genetic information, veteran status, marital status, and/or political affiliation in its programs, activities, or employment.