Policy Title

Restricted Data Security Policy

Policy Information

- Date issued: November, 2008
- Approved by: Chancellor's Cabinet
- Last revision: January, 2010

Reason for Policy

Identity theft continues to rise every year in the United States and the use of the Internet to steal sensitive data such as social security numbers (SSN's) and payment card numbers is a major contributor to this rise. Institutions of Higher Education have become attractive targets for Internet identity thieves because of their traditional dependencies on SSN's and open collaboration through distributed computer systems. Data credentials such as SSN's are used by thieves to setup fraudulent credit and perform other illegal activities associated with stealing a person's identity.

The implementation of an internally-generated Nebraska University ID (NU ID) at UNO has helped us take a big step forward in reducing the risk of data exposure, but routine daily use and electronic storage of SSN's, payment card numbers and other sensitive data is still pervasive on our campus. UNO has legal and ethical responsibilities to protect this sensitive data. Failure to do so could result in grievous 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 of 2006. This law outlines what must occur if unencrypted sensitive data, as defined in the Act, has been breached. In addition, UNO must meet Payment Card Industry Data Security Standards (PCI DSS) to properly secure payment card information. Failure to meet these standards could result in financial penalties and/or loss of ability to process payment cards at UNO.

As stewards of personal information, the University of Nebraska at Omaha has a responsibility to be vigilant and pro-active in the privacy of campus users *(see UNO Privacy Policy)* and the protection of restricted data that has been entrusted to our care. This policy serves to identify procedures and security requirements that must be met before authorization is granted to electronically store *Restricted Data*.

Definitions

Data Classifications

–Restricted Data
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.

–*Sensitive Data*
University data routinely used in conducting business and may be covered by State or Federal privacy law. It is protected to preserve the privacy, safety, or reputation of individuals and/or the University. Examples include student grades, birth dates, infrastructure maps, and donor contributions.

–*Public Data*
University data which are neither 'restricted' nor 'sensitive'. Generally, it 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.

Responsibilities

- ***Executive Restricted Data Authorization Committee*:** This committee consists of the Associate Vice Chancellor for Academic Affairs, Associate Vice Chancellor for Student Affairs, Associate Vice Chancellor for Technology and Associate Vice Chancellor for Business and Finance. They are responsible for reviewing decisions of the *Restricted Data Authorization Committee* as requested. The committee is responsible for the enforcement of this policy.
- ***Restricted Data Authorization Committee*:** This committee consists of the Director of Records and Registration, Director of Finance and Controller and Chief Information Security Officer. They are responsible for authorizing access to store *Restricted Data* and executing this policy.
- ***Data Users:*** *Data Users* are individuals authorized to access and electronically store protected data in execution of their job functions. Users are responsible for taking all reasonable measures to safeguard the confidentiality and integrity of protected data. 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 *Restricted Data Authorization Committee* in authorizing their staff's request to electronically store *Restricted Data*.
- ***ITS Cybersecurity Team:*** Responsible for enforcing technology requirements outlined in this policy.

Entities Affected By This Policy

All University personnel and entities.

Who Should Read This Policy

University personnel and entities that have access to and electronically store restricted data and/or collect, store and use personal information.

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

Restricted Data Storage

All personnel and entities associated with the University that intentionally store Restricted Data electronically are not authorized to do so beyond June 1, 2010, unless the procedures and security requirements outlined in this policy are met. 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 *Restricted Data* does not grant you permission to share that data with anyone. Electronic storage of *Restricted Data* is not permitted on non-University owned devices unless specifically authorized. **If you do not obtain authorization, then you must dispose of the data by following the secure deletion procedures outlined in the technical requirements referenced in the procedures section of this document.**

Risk Reduction and Enforcement

A technology device, called Vontu, has been installed on UNO's network to help reduce the risk of data breaches. *This device is intended ONLY to flag network traffic that contains unencrypted Restricted Data*. Vontu will also be utilized upon request, in coordination with primary campus technicians, to help faculty and staff identify where restricted data may unknowingly be stored at rest on devices.

The information found by Vontu is strictly used to reduce the risk of *Restricted Data* being breached. Access to reports generated by Vontu is authorized by the *Executive Restricted Data Authorization Committee* only for the use of enforcing this policy and reducing the exposure of restricted data. The use of Vontu complies with Executive Memorandum 16 and UNO's Privacy Policy.

Procedures

Requesting Access to Electronically Store Restricted Data

To be granted access to electronically store *Restricted Data*, you must first complete the request form located at:

http://its.unomaha.edu/cybersecurity/pdf/rdauthform.pdf

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 *Restricted Data Authorization Committee*. If authorization is granted, the *Restricted Data* approved must meet the storage requirements outlined below. In addition, reauthorization to continue to electronically store *Restricted Data* is required on an annual basis.

If a request is denied by the *Restricted Data Authorization Committee* and the requester believes they still need authorization to store such data, then the request goes before the *Executive Restricted Data Authorization Committee*. The *Executive Restricted Data Authorization Committee* will make the final decision.

Restricted Data Storage Requirements

Technical Requirements

ITS provides an electronic storage location for *Restricted Data* that meets the necessary technical requirements for those authorized to store it. If it is necessary to store your *Restricted Data* in an alternative location, you must explicitly state that on the Restricted Data authorization form.

Technical requirements must also be met to continue ongoing authorization to electronically store *Restricted Data*. The requirements are available on this website:

http://its.unomaha.edu/cybersecurity/pdf/rdtechreq.pdf

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

Devices authorized to store *Restricted Data* are subject to audits as deemed necessary by the *Restricted Data Authorization Committee*. You will be notified prior to when an audit would be performed and are required to cooperate fully with the resources performing the audit. Refusal to cooperate with an audit will be documented and reviewed by the *Executive Restricted Data Authorization Committee* for appropriate action.

Training

Training on technical requirements will be provided at the time authorization is granted to electronically store *Restricted Data* by Information Technology Services. Training must be completed before storage begins.

Policy Enforcement

This policy is enforced by the *Executive Restricted Data Authorization Committee* in coordination with Human Resources (Staff) and/or Academic Affairs (Faculty). Failure to comply with this policy may result in disciplinary actions.

References

Consumer Notification of Data Security Breach Act of 2006:

http://uniweb.legislature.ne.gov/FloorDocs/99/PDF/Slip/LB876.pdf