10-2014

# UNO Website: UNO Regulated Data Security Policy

University of Nebraska at Omaha

## Policy Title

Regulated Data Security Policy

## Policy Information

- Date issued: October, 2014
- Approved by: Chancellor's Cabinet
- Last revision: October, 2014

## 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. 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 University of Nebraska Omaha (UNO) has legal and ethical responsibilities to protect this sensitive data. Failure to do so could 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 of 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 could 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 pro-active in the protection of privacy of campus users and the protection of regulated 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 *Regulated Data*.

## Definitions

Data Classifications

–*Regulated Data*

University data that is highly confidential and is regulated by State or Federal privacy law. Unauthorized access to regulated data could result in 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 regulated 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.
- 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, or retina or 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 law. It is protected to preserve the privacy, safety, or reputation of individuals and/or the University.

*–Public Data*
University data which are neither "regulated" 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 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, and Associate Vice Chancellor for Business and Finance. They are responsible for reviewing decisions of the *Regulated Data Authorization Committee* as requested. The 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. They 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 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 *Regulated Data Authorization Committee* in authorizing their staff's request to electronically store *Regulated Data*.
- ***Information Security Office, Information Services:*** 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 regulated 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://is.unomaha.edu/policy/docs/rdauthform.pdf | Regulated Data Authorization form. |
| http://registrar.unomaha.edu/ferpa.php | UNO student records 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

### *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 A.*** 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 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 Executive Memorandum 16 and UNO's Privacy Policy.

## 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 or at: http://is.unomaha.edu/policy/docs/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 *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. Reauthorization to continue to electronically store *Regulated Data* is required on a biennial basis (should we put a timeframe such as "January"? maybe a two year process?)

Information Services 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* Storage Requirements

*Technical Requirements*

All regulated data must be stored on the Regulated Data Server managed by Information Services. 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 (ISO), Information Services*. Reasonable prior notification of an audit will be provided. Audit results are handled confidentially by ISO staff and 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 Information Technology Services. Training must be completed before storage 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.

## References

Consumer Notification of Data Security Breach Act of 2006:

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

# Appendix A

**University of Nebraska Omaha Regulated Data Standard**
Contact the Information Security Office at security@unomaha.edu for questions about this standard.

The university (University of Nebraska Omaha, UNO) engages in research, teaching, clinical, and business activities that encompass a variety of regulated data. This standard defines permitted and regulated uses of such university-owned data. This standard is governed by the following university policies:

**Scope and Authority**
This standard applies to all faculty, researchers, staff, students, and contractors of UNO. The Information Security Office, a division of Information Services, is responsible for the maintenance and interpretation of this standard.

**Standard**
Members of the university community have an individual and a shared responsibility to:

- Maintain university-owned regulated data only in the environments permitted by this standard.
- *Never maintain university sensitive regulated data on personally-owned devices or via personally-maintained services;*
- Report a violation of this standard, whether intentional or unintentional, as an information security incident per Information Security Incident Reporting Policy to security@unomaha.edu within 24 hours.

**Definitions**
Regulated Data: For purposes of this standard, "regulated data" is defined as data that requires the university to implement specific privacy and security safeguards as mandated by federal, state, and/or local law, or university policy or agreement. Regulations or categories of data most applicable to UNO include:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Social Security Numbers (SSNs)
- Gramm Leach Bliley Act (GLBA)
- Payment Card Industry Data Security Standards (PCI-DSS)
- Sensitive Identifiable Human Subject Research
- Export Controlled Research - International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)

The University of Nebraska has defined the following student information as public directory information:

- student name
- local address
- permanent address
- telephone listings
- year at the University
- dates of attendance
- academic college and major field of study
- enrollment status (e.g. undergraduate or graduate; full-time or part-time)
- participation in officially recognized activities and sports
- degrees, honors and awards received

**IT Environment:** For purposes of this standard, "IT environment" means any IT service directly maintained by the university, under contract or agreement with UNO, or that is personally-owned or maintained but is used for university business.
**University-owned:** For purposes of this standard, "university-owned" data means any data that is created or maintained under the auspices of an individual's institutional role as a university employee or affiliate.
**Personally-owned:** For purposes of this standard, "personally-owned" means any device, mobile or otherwise, or service that is not governed by a university contract or agreement.

# Appendix B

## Regulated Data Authorization Form

*Please complete the form below and return to UNO Information Services (IS) Technical Support Services, EAB 104.*

Date: _____

**1. Your Information**

Name: _____

Phone: _____

Email: _____

NU ID: _____

College/Department _____

Dean/Divisional Leader _____

**2. Storage Device Information**

*(Submit one form per device)*

IS provides a service for the storage of *Regulated Data,* known as the Regulated Data File Server, which meets the necessary technical requirements for those authorized to store it. If it is necessary to store your *Regulated Data* in an alternative location, you must explicitly state that below:

☐ If authorized, I will store *Regulated Data* on the Regulated Data File Server. (if checked, please proceed to section 3)

☐ If authorized, I will **NOT** store Regulated Data on the Regulated Data File Server. Please state your reason and location where you would like to store *Regulated Data*:

Reason: _____

*Location:*

☐ Server IP: Hostname: _____

☐ Workstation
☐ Laptop
☐ Other _____

Location of Device: Building: _____ Room: _____

Owned by: □ UNO □ Self □ Other_____

Technical Support Staff Information:
*If the device is UNO owned and is a workstation, laptop, usb drive, etc, then your primary technician must sign below to acknowledge your storage of Regulated Data. You as the user of this device are responsible for the security of the Regulated Data on it.*

**Regulated Data Storage Technical Requirements**

*Technical Requirements*

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

The following technical requirements must be met once you are authorized to store regulated University data.

**If you are storing Regulated Data on the IS managed Regulated Data Storage System, the device (laptop, workstation, etc) being used to access the data must meet the following requirements:**

- Software patches: Auto updates must be enabled or critical patches must be applied within a timely manner of being released. If a critical update cannot be applied, then you must notify the ISO at security at unomaha.edu
- Current anti-virus and spyware software must be enabled and set to scan and receive definition updates daily.
- Local firewalls must be enabled and only allow necessary network traffic.
- When possible, devices such as servers, workstations and laptops used to store Regulated Data or access it on the Regulated Data Storage System must use strong 128bit encryption.
- Workstations, laptops, servers, portable devices and any other devices used to electronically store Regulated Data or access it on the Regulated Data Storage System are subject to audits to ensure technology requirements are being met as deemed necessary by the *Regulated Data Authorization Committee*.
- Once a device is no longer being used by the person authorized to store Regulated Data on it or access data on the Regulated Data Storage System, a complete secure deletion of the device must be done by or through the Information Security Office.

**If you are NOT storing Regulated Data on the IS managed Regulated Data Storage System, the device (laptop, workstation, etc) being used to store must meet the following requirements, *in addition to the requirements listed above*:**

- Regulated Data cannot be stored on a device that directly accepts incoming connections from the Internet, such as a web server or other forward facing service.
- The server will use Identity Finder to accurately inventory the contents of the system.
- Vulnerability scans will be performed on a regular basis on workstations and servers storing Regulated Data by the ISO. Critical issues identified in the scan must be acted upon in a reasonable timeframe as deemed by the ISO.
- Reasonable protective measures must be put in place to physically secure devices that store Regulated Data. These measures should prevent easy physical theft.
- Deletion of Regulated Data must be done using a secure deletion tool

*If the device that you use to store Regulated Data on is a server, then the primary technician for that server is responsible for the security of the data on that device.*

By signing below I acknowledge that the requester is storing *Regulated Data* on a device in the area that I support. If the device is a server I manage, then I understand that I am responsible for protecting the *Regulated Data* on it.

Primary Technician Support Staff Signature: _____

Phone: _____ Email: _____

**3. Regulated Data File Server Authorization**

If seeking authorization to store *Regulated Data* on the IS-managed Regulated Data File Server, please complete the following section.

Department Name: _____
(this or a similar name will become the folder name on the Regulated Data File Server and the Active Directory group name which protects this folder)

Users (UNO NetIDs) authorized to access this folder: _____

_____

Person(s) Authorized (UNO NetIDs) to request membership changes to the Group protecting this folder:

_____

**4. Regulated Data Type**
*(Check all data types stored on the device. Report only University-owned Regulated Data. For example, if you store your own credit card information on your laptop, it does not apply.)*

☐ SSN

☐ Bank Account Access *(bank account numbers, credit card numbers, etc)*

☐ Driver's/State License #

☐ Username with Password *(username/ID number in combination with password/PIN that grants access to Regulated Data)*

☐ Biometric Information

**5. Can the device (laptop, workstation, etc) being used to store *Regulated Data* OR access *Regulated Data* on the IS managed Regulated Data File Server be encrypted?**

☐ Yes ☐ No If no, please explain the reason here

## 6. Your Business Need

*(Please indicate your need to store this data)*

## 7. 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://is.unomaha.edu/pdf/rdauthform.pdf | Regulated Data Authorization form |
| 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) |

## 8. Employee Responsibilities

*(The following is the list of terms and conditions related to the electronic storage of regulated University Data)*

_____ I understand that I am responsible for protecting the *Regulated Data* that I electronically store.
*(initials)*

_____ I agree to receive training on how to securely store *Regulated Data*.
*(initials)*

_____ I agree to report all security violations to my supervisor immediately.
*(initials)*

_____ I understand that any violation of this agreement may be cause for disciplinary and, possibly, legal action
*(initials)*

_____ I understand I will be subject to annual reauthorization which includes re-submission of this form on an annual basis.
*(initials)*

**Employee:**

By signing below, I am acknowledging that I have read and agree to the terms and conditions described in this form and I have read and agree to comply with the University policies governing the use, storage, and disposal of *Regulated Data*.

Signature Date

**9. Authorization**

**Dean/Divisional Leader:**

This employee should be authorized to store *Regulated Data* on an electronic storage device as a necessary part of his/her job duties.

Signature Date

**Regulated Data Authorization Committee:**

**Signature** **Date**

☐ **Approved**

☐ **Denied for reason:**