University of Nebraska
LINCOLN | OMAHA | KEARNEY | MEDICAL CENTER

Effective: 12/31/17
Last Revised: 8/28/17

Responsible University Administrator:
Vice Chancellor for Information Services & CIO

Responsible University Office:
Information Technology Services

Policy Contact:
Chief Information Security Officer,
security@nebraska.edu

ITS-05 Data Classification and Management Policy

Scope

This policy applies to all University of Nebraska (University) personnel including all faculty, staff, students, contractors, consultants or other entities that collect, store, have access to, or use personal information in any university provisioned network.

Policy Statement

All personnel and entities associated with the university that intentionally store high risk data (refer to definition below) electronically are required to seek authorization from the Information Security Office prior to storing. 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 permission to share that data with anyone. Electronic storage of restricted data is not permitted on non-university owned devices unless specifically authorized. You must contact the Information Security Office for assistance in disposing any restricted data.

Parties that are storing medium risk data are recommended to contact the Information Security Office to further discuss its proper storage.

Risk Reduction and Enforcement

Data scanning software for data loss prevention (DLP) has been installed on the University of Nebraska's (NU) network and endpoints to help reduce the risk of data breaches. This software is intended only to flag network traffic and data storage that contains unencrypted restricted data. The information found by the DLP software is strictly used to reduce the risk of restricted data being breached. Access to reports generated by DLP software is by authorized security personnel only. The use of DLP software complies with NU Executive Memorandum 16 and Executive Memorandum 26.

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 or account 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. NU 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 University is subject to multiple regulations and laws relating to the access to and management of information. These include LB 835 Data Breach Reporting, Payment Card Industry (PCI) Standards, the Health Insurance Portability and Accountability Act (HIPAA) and Graham Leach Bliley Act (GLBA) to name a few.

Procedures

A. **Requesting Access to Electronically Store Restricted Data**

1. To be granted access to electronically store restricted data, you must first contact the Information Security Office to inventory the data.

2. If a restricted data storage request is denied the requester may appeal to the decision to the VP of IT and CIO. Reauthorization to continue to electronically store restricted data is required on a biennial basis.

3. Information Technology Services (ITS) provides approved storage for any authorized individual or department to use. If the approved storage will not be used, the proposed storage location must be an ITS data center or have received approval from the Information Security office after an audit of the system's ability to meet the stringent requirements ITS requires.

B. **Exception Process**

1. If it is expected that if the data will not be stored in an ITS data center or on ITS approved equipment, the support person shall submit an Exception Request to security@nebraska.edu

2. All efforts shall be made to ensure data is managed within an ITS data center. However, if it is not feasible to move the data or manage it in an ITS data center, an exception request may be granted.

3. Disagreements will be escalated to the NU Data Governance Council.

4. The Information Security Office will maintain all documentation regarding all exception requests

5. All high risk data must be stored on a server or on an approved service managed by ITS. Updates will continue to be made to these requirements as technology and cybersecurity threats change. Authorized users will be notified as changes are made.

6. It is recommended that al medium risk data to be stored on ITS systems and if it is not it is recommended that you consult the Information Security Office.

C. **Audits**

1. All university-owned equipment is subject to audit for unauthorized storage of restricted data. Devices authorized to store restricted data are subject to audits as deemed necessary by the

2. 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 Restricted Data Authorization Committee in aggregate.

D. **Training**

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

E. **Policy Enforcement**

1. This policy is enforced by the Chief Information Security Officer. Failure to comply with this policy may result in disciplinary actions.

Definitions

A. **High Risk Data (Restricted use)**: University data that is highly confidential and is restricted by international, state or federal privacy laws. The loss of confidentiality, integrity, or availability of the data or system could have a SEVERE adverse impact on our mission, safety, finances, or reputation and is subject to state or federal privacy or breach reporting laws Other information that presents a significant competitive or regulatory disclosure risk including, but not limited to, intellectual property subject to a confidentiality obligation, Homeland Security information, Social Security Numbers, data related to University Police and Internal Audit investigations, and data that describes University network and computing configurations and security controls.

1. Specific examples of restricted data include:

1.a. Social Security Numbers

1.b. Motor vehicle operator's license number or state identification card number

1.c. 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

1.d. Student records (except those defined by university policy as directory information under FERPA)

1.e. Unique electronic identification number, username, or routing code, in combination with any required security code, access code, or password

1.f. Unique biometric data such as fingerprint, voice print, retina/iris image, or other unique physical representation

1.g. Email address or id with a password or security question

1.h. Controlled classified information in regards to specific research.

B. **Medium Risk Data**

1. Electronic data requiring high levels of protection due to the following circumstances:

1.a. Data collected is subject to management under filed research data management plans.

1.b. Data received or collected must be protected under specific requirements of externally-supported research agreements.

1.c. The project under which the data is being collected carries a security classification established by an authorized agency of the federal government.

1.d. Information or data collected would violate the confidentiality of sources or subjects involved in the research.

1.e. Other instances where data collected warrants additional protection due to contractual agreements or other written agreed upon conditions.

1.f. Examples:

1.f.a. Sensitive digital research data

1.f.b. University internal ID's or numbers that are not public record but are used for internal operations such as cost center numbers, network diagrams, or other information considered to be private but not regulated.

C. **Low Risk Data**: University data routinely used in conducting business not covered by international, state or federal privacy and security laws. The data are protected to preserve the privacy, safety, and reputation of individuals and/ or the university. University data which are categorized as neither "restricted" 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. Data which is required to be disclosed under public records laws.

1. Further evaluation can be compared against the following framework from NIST 800-60 Rev1.

D. **Data Users**

1. Data Users are individuals authorized to access and electronically store restricted 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.

E. **Academic Deans and Divisional Leaders**

1. 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.

Contacts

Information Security Office – security@nebraska.edu

Related Information

Executive Memorandum 16 (links to be added)

Executive Memorandum 26 (links to be added)

ISO 27002 (links to be added)

NIST-800-53 (links to be added)

Nebraska Statute LB 835 2016 (links to be added)

History

Created by Matt Morton

edited by Erin Busch

124 Edited by Michael Justus

125 Edited by Matt Morton, Risk Haugerud, Andrea Childress