Effective: *February 14, 2019*
Last Revised: *February 13, 2019*

Responsible University Administrators:
Vice President for Information Technology
Executive Vice President and Provost

Responsible University Office:
NU ITS Cybersecurity

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

Data Classification and Storage Policy

ITS-05

POLICY CONTENTS

Scope

This policy applies to all University of Nebraska (University, NU) personnel including all faculty, staff, students, contractors, consultants, or other entities that collect, store, or have access to institutional data in University provisioned systems and networks. Parties working in units supported by NU affiliates should use the most restrictive data classification scheme. Refer to the Data Classification and Use Matrix (https://its.nebraska.edu/policies-processes/DataUseMatrix.pdf) for questions on specific data classifications and restrictions related to storage and transfer.

Policy Statement

All personnel and entities associated with the University that store high or medium risk data electronically are required to seek authorization from the NU ITS Cybersecurity Office before storing high or medium risk data. Authorization to electronically store high risk data does not grant permission to share that data with anyone. Electronic storage of medium or high risk data is not permitted on personal devices unless specially authorized via the exception process outlined below. All parties wishing to dispose of medium or high risk data should contact the NU ITS Cybersecurity Office for assistance with this task.

Data stewards are required to classify their data upon receipt and resolve any concerns by referencing the Data Use Matrix (https://its.nebraska.edu/policies-processes/DataUseMatrix.pdf). All classifications will be reviewed and are subject to final approval through the Data Classification procedure. Any data that cannot be classified or for

which there are questions on its storage, the user should contact the NU ITS Cybersecurity Office for clarification.

This policy also applies to third parties that provide services to the University and those releases required by law (e.g. financial aid and payroll). Anyone wanting to share medium or high risk data with third parties should have prior authorization and have completed a formal data sharing agreement. Such an addendum or agreement will be reviewed by the NU Office of the Vice President and General Counsel. Templates are available from the General Counsel's office.

Parties who are storing high, medium, and low risk data should also follow the minimum-security standards to further understand its proper storage and disposal. The NU minimum-security standards are located here: https://its.nebraska.edu/minimum-security-standards.php

Reason for Policy

The Data Governance Council commissioned by the University of Nebraska President, a working committee, was formed with the primary purpose to develop policy to protect institutional data while preserving the open, information-sharing mission of the University's academic cultures. Institutional data is classified in accordance with legal, regulatory, administrative, and contractual requirements; intellectual property and ethical considerations; strategic or proprietary value; and/or operational use. In addition,

- It is important that high and medium risk data are secured properly to protect the privacy of individuals and the data assets of the University of Nebraska; and,

- The University is subject to multiple regulations and laws relating to the access to and management of information, including, but are not limited to, Nebraska's Financial Data Protection and Consumer Notification of Data Security Breach Act, Payment Card Industry (PCI) Standards, the Health Insurance Portability and Accountability Act (HIPPA), Family Educational Rights and Privacy Act (FERPA), Graham Leach Bliley Act (GLBA), and European Union's General Data Protection Regulation (GDPR).

Definitions

Data Classifications: The following outlines high, medium, and low risk data classification as well as where to find the minimum security requirements to protect that data. There are three classification levels of institutional data:

> **High Risk Data (Confidential and Highly Restricted):** High risk data is institutional data that is highly confidential and covered by international, state, or federal privacy laws. Data where 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, or is subject to international, federal, or state privacy or breach reporting laws.

Data is considered high risk if:

- The data is highly confidential, and protection of the data is required by law/regulation; or,
- The University is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed; or,
- The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Medium Risk Data: Medium risk institutional data is data requiring high levels of protection due to the following circumstances:

- Protection of the data is required by law/regulation; or,
- Data received or collective is subject to contractual confidentiality provisions; or,
- The data carries a security classification established by an authorized agency of the federal government; or,
- The loss of confidentiality, integrity, or availability of the data or system could have a negative impact on our mission, finances, or reputation.

Low Risk Data: Institutional data routinely used in conducting business not covered by international, state, or federal privacy and security laws. 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.

NOTE: Institutional data belonging to any classification level may be subject to Nebraska public records laws. Please contact the campus records officer or the NU Office of the Vice President and General Counsel immediately upon receipt of a public records request.

Institutional Data: Institutional Data is information created, collected, maintained, transmitted, or recorded by or for the University to conduct University business. It includes data used for planning, managing, operating, controlling, or auditing University functions, operations, and mission. Institutional data includes, but is not limited to, information in paper, electronic, audio, and visual formats. Institutional Data does not include data used in pursuit of research. Further, it does not include personal data which is information created, collected, maintained, transmitted, or recorded by University-owned devices, media, or systems in accordance with Executive Memorandum No. 16 that is personal and not related to University business.

Responsible Party: Individual or group of people that are responsible for a decision or action.

Data Classification and Use Matrix: Defines the appropriate data classification levels for institutional data elements and identifies which classifications of institutional data are permitted for specific data user's activities.

Data Stewards: Data Stewards are subject matter experts and operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for that area and its related Institutional Data. Data Stewards

within a campus are assigned by senior operational managers responsible for implementing policies within each functional area.

Verification: An evaluation of an organization's information technology infrastructure, policies, and operations. Information technology reviews to determine whether IT controls protect corporate assets, ensure data integrity, and are aligned with the goals of the University.

Procedures

Data Classification: Classification of data elements if facilitated by the Institutional Data Classification, Use, and Policy Committee. Data classification is applied to any new or existing system, application, or service that is utilized for managing, consuming, or storing institutional data. Classifications should be reviewed annually by the Data Stewards and classifications are reviewed at least annually through manual and automated system inspections by the Chief Information Security Officer or their designee.

Exception Process:

1. Electronic storage of high or medium risk data is not permitted on non-University-owned devices unless specifically authorized. Limited exceptions to this requirement may be granted in extraordinary circumstances. Responsible parties desiring an exception should submit an Exception Request to its-sec@nebraska.edu.

2. In the event that an Exception Request is denied, the responsible party may appeal by sending an email to its-sec@nebraska.edu. The responsible party needs to demonstrate that all efforts to store and manage data within a NU ITS data center or on NU ITS approved equipment were unsuccessful. The NU Executive Vice President and Provost will have final decision-making authority over all appeal requests.

3. The NU ITS Cybersecurity Office will maintain all documentation regarding all exception requests.

Verification and Risk Reduction: All University equipment is subject to review for verifying classification and proper storage of high risk data. Devices authorized to store high risk data are subject to reviews as deemed necessary by the NU ITS Cybersecurity Office. Responsible prior notification of a review may be provided depending upon circumstances. The NU ITS Cybersecurity Office frequently scans data and reviews traffic on the University network and endpoints to help reduce the risk of data breaches and material harm to the University. Access to reports generated by the NU ITS Cybersecurity Office is limited to authorized personnel and internal or external auditors only. This complies with Executive Memorandum Nos. 16 and 26.

Training: Security training on the technical requirements of this policy will be provided at the time authorization is granted to electronically store medium and high risk data. Security training will be required for all parties prior to their access to and use of high risk data.

Policy Enforcement: This policy is enforced by the Chief Information Security Officer. Failure to comply with University IT policies may result in sanctions related to the individual's use of IT resources or other appropriate sanctions via University personnel and student policies.

Provisioned: Provided by or managed by the University of Nebraska and its affiliates.

Review: This policy will be reviewed annually by the Chief Information Security Officer.

Contacts

NU ITS Cybersecurity Office: its-sec@nebraska.edu

Forms

Authorization Form
Exception Request Form
Exception Appeal Request Form

Related Information

Executive Memorandum No. 16
Executive Memorandum No. 26
Neb. Rev. Stat. §§ 87-801 to 87-808
NIST 800-53
NIST 800-171
NIST CSF
NIST 800-60 Rev1
ID-01: Data Use Policy

History

February 13, 2019 Approved by President's Council