UNIVERSITY OF SOUTH DAKOTA

Policy Number: 5.003
Originating Office: Information Technology Services
Responsible Executive: Chief Information Officer
Date Issued: 12/08/2010
Date Last Revised: 10/01/2024

Information Security and Data Responsibilities

POLICY CONTENTS

I. REASON FOR THIS POLICY

The university is required to protect its information technology resources, complying with applicable laws and regulations, and adhering to South Dakota Board of Regents (SDBOR) policies for the integrity, protection, and preservation of systems and data. This policy will be evaluated on an annual basis to ensure its adequacy and relevancy regarding The University of South Dakota's (USD's) needs and goals.

II. STATEMENT OF POLICY

USD employees must responsibly use university information technology resources and take appropriate measures to secure them and the data they contain, in compliance with university and SDBOR policies, requirements, and best practices.

III. DEFINITIONS

Employee Facing Technologies: Information technology resources and devices used by employees in the performance of their job duties. These include, but are not limited to, desktop computers, laptop computers, tablets, credit card machines, smartphones, cloud services, storage systems, virtual environments, and devices or systems listed in Board of Regents Acceptable Use of Information Systems Policy 7.1

Data Classifications:

- **Public Data:** Information intended for public use or information that can be disclosed without significant risk to USD or the SDBOR. Unauthorized disclosure, alteration, or destruction has low or no financial or reputational impact.

- **Internal Data:** Information intended for use within the university that, if disclosed, would not result in significant harm but is not intended for public dissemination. Unauthorized disclosure, alteration, or destruction could have a moderate financial or reputational impact on USD or the SDBOR.

- **Restricted Data:** Sensitive information that requires strict controls due to legal, regulatory, or policy requirements. Unauthorized disclosure, alteration, or destruction could have criminal or extreme financial or reputational impact on USD or the SDBOR.

By default, all university data is considered Internal unless classified otherwise.

ITS Security Safeguards: A comprehensive set of security measures implemented by the Information Technology Services (ITS) department to safeguard university data and IT resources. These include, but are not limited to, Endpoint Detection and Response (EDR), DNS Security, Artificial Intelligence (AI) Security, Network Security, Data Loss Prevention (DLP), Encryption, Multi-Factor Authentication (MFA), Application Restrictions, Computer Administrator Restrictions, and Email Security.

IV. PROCEDURES

User Responsibilities

A. Compliance and Training:
   1. Comply with information security guidelines and practices established by the University USD and the SDBOR.
   2. Understand and comply with current policies, requirements, guidelines, procedures, protocols, and regulations concerning the security of the university's electronic resources and data.
   3. Complete annual security awareness training.
   4. Complete role-specific training is required.

B. Data handling:
   1. Ensure that personally identifiable information is not sent or shared unencrypted over email, instant messaging, chat, forums, or any other end-user messaging technologies.
   2. Enter or access sensitive data only on, or with, employee-facing technologies that are properly secured with ITS security safeguards.
   3. Store and share university data only in approved storage locations that meet the university's security requirements and only share via approved methods.

4. Handle data covered under regulations such as FERPA, GLBA, HIPAA, PCI, etc., responsibly, adhering to all applicable laws, SDBOR, and university policies.
5. Use only approved AI technologies when working with restricted data, ensuring compliance with data protection standards. The use of restricted data requires appropriate approval, inventory, and auditing.
6. We encourage the use and experimentation with generative AI; however use of restricted USD data is prohibited without prior authorization.

C. Device Security:
   1. Ensure all USD-owned devices are encrypted by ITS using standard drive encryption software, if supported, to prevent unauthorized access in the event the device is lost or stolen.
   2. Remote work requires the use of approved remote access tools, equipment, and methods approved by the SDBOR.
   3. Report all electronic or physical device-based security incidents to the ITS Service Desk immediately.

Failure to comply with these responsibilities or attempts to circumvent security safeguards may result in disciplinary action, up to and including termination.

ITS Security Officer Responsibilities

A. All responsibilities in the user and ITS staff responsibility sections.
B. Develop a comprehensive cybersecurity program that includes risk assessment, data protection, systems protection, best practices, and education.
C. Create and distribute security incident response and escalation procedures.
D. Assist or lead cybersecurity and data incident resolution for the university and individual units.
E. Develop, implement, and support ITS security safeguards, monitoring, and analysis.
F. Monitor and analyze security alerts and distribute information to appropriate personnel.
G. Support and verify compliance with federal, state, and local legislation as well as industry standards.

ITS Staff Responsibilities

A. General Responsibilities

   1. All responsibilities listed in the user responsibility section.

B. Knowledge and Compliance

   1. Be knowledgeable and comply with current policies and procedures concerning the security of the university's information technology resources and data.

C. Device Management

1. Understand and document the specific configurations and characteristics of the IT devices they support to respond to emerging technology threats and support security event mitigation efforts.
2. Ensure device and system encryption is in place on employee-facing technologies.
3. Ensure that all employee-facing technologies are installed in the correct network location and all ITS security safeguards are in place.
4. Ensure that the principle of the least privilege is used when granting access to IT devices, systems, and services.

D. Security Measures

1. Recommend and implement appropriate security measures for resources under their control.
2. Maintain and deliver the most recent information system patches and updates available.
3. Maintain and deliver current and available security configurations.
4. Maintain and secure password configurations on all IT devices and services, changing all default or administrative passwords.
5. Ensure all enterprise systems have appropriate security safeguards in place.

E. Data Protection

1. Build and maintain technical implementations to inventory, classify, and protect data.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Board of Regents Acceptable Use of Information Systems Policy 7.1
Board of Regents Alternative Work Schedules & Remote Work Arrangements Policy 4.1.5
Board of Regents Personally Identifiable Information Policy 7.7
USD Data Classification Categories
USD Incident Handling Policy 5.004
USD IT Security Program and Policies