MONTANA BOARD OF REGENTS OF HIGHER EDUCATION
Policy and Procedures Manual

SUBJECT: INFORMATION TECHNOLOGY
Policy 1300.1 - Security of Data and Information Technology Resources; Montana University System
Adopted: November 16, 2001; Revised: May 23, 2014; Revised November 18, 2022

I. Board Policy`

The purpose of this policy is to establish fundamental principles governing the security of data and information technology across the Montana University System (MUS) and to ensure compliance with pertinent federal and state laws, rules, regulations, and other requirements. Under § 20-25-301, MCA, the Board of Regents shall ensure an adequate level of security for data within the university system.

II. Responsibilities

A. Information technology leadership at affiliated campuses shall report functionally to the flagship chief information officer (CIO) and administratively to campus management. Flagship CIOs are responsible for information security across the affiliation and have the authority to assign security roles across the affiliation in support of this policy.

B. Flagship CIOs, in coordination with the flagship presidents and the Office of the Commissioner of Higher Education (OCHE), shall establish appropriate management and governance structures related to MUS information security. OCHE will maintain security and information technology governance requirements and post them to the MUS website.

C. At least annually, each flagship CIO will advise and inform the Board of Regents on the overall status of and compliance with the information security program and standards.

~~A.~~D. ~~A.~~ Each campus of the ~~Montana University System~~ (MUS) ~~is required to~~ must establish and maintain policies for the security of data and information technology resources under its control.

E. Campuses shall develop and maintain policies under the direction of the affiliated flagship CIO. The CIO at each flagship shall assign to appropriate individuals or groups the responsibility for development of policies governing the security of data and information technology resources that specifically encompass the responsibilities outlined in MCA 2-15-114.

~~B. Policies shall be developed and maintained under the direction of the chief executive officer of each campus.~~

~~B. Policy Review~~

F. ~~Periodically, no less often than every three years,~~ Flagship CIOs or the CIO's delegates, shall review campus policies for the security of data and information technology resources ~~shall be reviewed~~ as established by campus policy or as defined by other compliance requirements. ~~by the chief executive officer of the campus and/or his/her delegates. Revisions shall be undertaken when judged necessary, following the procedure outlined above.~~ The CIO at each flagship, and/or the CIO's delegate, shall coordinate with internal and external evaluators to ensure regular assessments of the security program are conducted.

G. OCHE shall develop and maintain policies for the security of data and information technology resources under its direct control.

MONTANA BOARD OF REGENTS OF HIGHER EDUCATION
Policy and Procedures Manual

SUBJECT: INFORMATION TECHNOLOGY
Policy 1300.1 - Security of Data and Information Technology Resources; Montana University System
Adopted: November 16, 2001; Revised: May 23, 2014; Revised November 18, 2022

III. Standards for Security Controls

~~C~~A. Policies shall comply with all pertinent state, ~~and~~ federal, and other requirements. ~~Where appropriate,~~ C~~c~~ampuses ~~should~~ shall adopt ~~follow~~ the National Institute of Standards and Technology (NIST) Cybersecurity Framework for policy guidance. ~~The~~ The Framework complements, and does not replace, a campus's risk management process and ~~cyber~~security program. Where appropriate, exceptions to the Framework should be documented and approved by the affiliated flagship CIO. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of ~~cyber~~security risk while aligning with industry practices.

B. ~~D.~~ Campuses ~~policies~~ must ~~include a security~~ develop and maintain an incident response plan to ensure that IT security incidents are properly reported, documented, and resolved/remediated. ~~In~~ In the event that a security incident requires public disclosure, the Commissioner of Higher Education ~~will~~ must be notified prior to the disclosure.

~~E. Insofar as security issues are common to campuses, the campuses shall adopt similar policies.~~

~~F. The Office of the Commissioner of Higher Education shall develop and maintain policies for the security of data and information technology resources under its direct control.~~

~~II. Procedures~~

~~A. Policy Development~~
~~1. The chief executive officers of each campus shall assign to appropriate individuals or groups the responsibility for development of policies governing the security of data and information technology resources that specifically encompass the responsibilities outlined in MCA 2-15-114. Those individuals or groups shall engage their campus communities in the identification of security issues and exposures and shall develop draft policies reflecting those concerns.~~
~~2. The chief executive officer shall review and approve the campus security policy.~~

~~B. Policy Review~~
~~1. Periodically, no less often than every three years, campus policies for the security of data and information technology resources shall be reviewed by the chief executive officer of the campus and/or his/her delegates. Revisions shall be undertaken when judged necessary, following the procedure outlined above.~~

Definitions:

A. *Security* means the ~~p~~Prevention of unauthorized additions, deletions, or modifications to data; prevention of unauthorized access to sensitive or confidential data; protection of the accuracy of data; protection of the privacy or confidentiality of sensitive data; protection against unauthorized access to information technology resources; and protection of information technology resources from intrusion, damage, denial of service, or other disruption.

SUBJECT: INFORMATION TECHNOLOGY
Policy 1300.1 - Security of Data and Information Technology Resources; Montana University System
Adopted: November 16, 2001; Revised: May 23, 2014; Revised November 18, 2022

B. *Data* means ~~–~~ r~~R~~ecords (physical, electronic, optical, etc.) detailing or summarizing the financial, human resources, financial aid, or student records aspects of the entities of the ~~Montana University System~~ MUS Information Technology Resources. Data includes voice ~~– Voice~~, data, and video networks and associated electronic equipment; computers; storage devices; databases; application software; and operating systems.

~~*A.*~~ *C.* Administrative reporting means a direct line of authority within the campus organizational hierarchy which includes human resource related activities.

~~*B.*~~ *D.* Functional reporting establishes a connection between flagship CIOs and IT leadership across the affiliation based on the specialized nature of the IT function for which responsibilities related to IT governance and information security are shared.

History:

Legislative Audit Division report on The University of Montana, April 1999, *Draft, July 27, 2001, Draft August 23, 2001;* ITEM 112-110-R0901 - Security of Data and Information Technology Resources; Montana University System; approved November 16, 2001. Item 163-105-R0514, revised May 23, 2014. Revised November 18, 2022, Item 203-106-R1122.