MONTANA UNIVERSITY SYSTEM

OCHE IT Governance Project

Office of the Commissioner of Higher Education | 560 N. Park Ave. PO Box 203201
Helena, MT 59620 | (406) 449-9124 | www.mus.edu

Background

The governance and administration of the MUS are vested with the Board of Regents (“Board”), which has the full authority to manage and control the MUS. The MUS gathers and stores various types of sensitive information related to students’ education and personal information, employees’ personal information, credit and bank account information, intellectual property, and personal health information. The MUS also stores information that is subject to federal security requirements. Montana state law also requires certain activities for maintaining information security. The Board and OCHE are responsible for governing IT management practices and information security throughout the university system.

A recent legislative audit recommended Board of Regents and universities review and enforce university system security policy that includes:

A. Clear direction within policy to manage a security program and mandate a consistent security framework, going above and beyond maintaining security policies; and
B. Requirements for Board of Regents security policy to be reviewed continuously.

The audit also recommended the establishment of system-wide IT governance that ensures:

A. OCHE has an active role in improving security posture of the university system,
B. Security policy addresses the requirements of data security statute and other relevant federal requirements,
C. There is clear allocation of security responsibility, authority, and accountability; and
D. Communication and reporting mechanisms are formalized between various entities that oversee or make decisions within the university system.

High Level Scope

The purpose of this project is to understand the MUS business context, the resources that support critical functions, and the related information security risks. This process will help further develop the Board’s IT governance structure.

OCHE will establish a workgroup comprised of the Commissioner’s staff and university system stakeholders to identify and analyze security frameworks and their applicability to the MUS. Based on the recommendations of the workgroup, OCHE will recommend to the Board of Regents a governance approach that will ensure security controls are implemented across the MUS in a manner that will most effectively protect sensitive MUS information.

Business Need/Project Objectives

1. Increase MUS information security knowledge base at OCHE
2. Comply with state and federal laws
3. Revise IT governance policy and improve communication to the BOR
4. Provide ongoing leadership and coordination in furtherance of IT governance practices

Project Approach

The project will follow a traditional approach with established milestones and completion dates.

Project Timeline

Start Date: 5/01/2022
End Date: 5/31/2023

Project Milestones/Deliverables

Milestone/Deliverable	Estimated Completion Date
Project Charter developed	5/1
Develop MUS information security template and identify gaps	7/30
Review of applicable IT governance frameworks	8/31
Identify shared services (i.e., risk assessment, security information and event management)	9/30
Draft BOR policy	11/4
Final approval BOR policy	1/2/23
Ongoing monitoring and system security program development	Move to monthly/quarterly check-ins

Key Stakeholders

Sponsor	BOR/Tyler Trevor, Deputy Commissioner for Budget & Planning, Chief of Staff
Project Manager	Margaret Wallace, Director of Assurance and Enterprise Risk
Project Team Members	John Thunstrom, Justin Van Almelo, Zach Rossmiller, Jonathon Neff, Ryan Knutson, Adam Edelman, Jessica Weltman, Camie Bechtold, Ila Saunders, Anta Coulibaly
SME's	CIOs/CISOs/VPs of Research/Auditors
Others impacted	Affiliated campuses, legal & compliance experts, students

Estimated Effort

Role	Overall Responsibility	Estimated Effort (hours)
Sponsor	• Champion the project • Resolve external barriers • Stay informed • Approve/deny scope changes	10%
Project Manager	• Manage the project	30%
Project Team Members	• Participate in the tasks involved with the project	15%
SME's	• Subject Matter Expert for project	15%

Constraints, Assumptions, Risks

Constraints	• Resources available for the project
Assumptions	• Dedicated project team members
Risks	• Resource Capacity • Timeframe