Information Security Risk Management Policy (ISP-04)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to the IT department and business departments.

Table of Contents

Introduction

A risk management process and assessment that delivers a holistic and systematic approach to risk management is a critical part of an effective Information Security Management Plan. It is also mandated by the FTC Safeguards rule which itself is required by the Department of Education. The goal of the risk assessment is to identify, categorize, and prioritize remediation of risks to achieve business alignment. This enables work to be effectively triaged to deliver the best results, i.e. maximum risk reduction, at an optimum cost.

Put another way Risk Management is about making the most of the information that you have available to reduce the likelihood and impact of incidents and continually improving that information over time.

Objective

The objective of this policy is to define how IT security risk will be managed at the University. This includes the risk identification, assessment, mitigation, and ongoing management as part of the Universities Information Security Management Plan. Additionally, the roles and responsibilities will be defined.

Policy Statement

General

The risk management process consists of four parts:

1. Identification of Universities assets and services
2. Identification of control and system vulnerabilities or weaknesses and likely threats that could exploit them to establish a risk
3. Identification of Mitigating measures or control improvements
4. Prioritization of the improvements based on risk removal

At least once a year this process is repeated following the classic Deming Quality Improvement Cycle of Plan, Do, Check, Act, cycle or the NIST Categorize, Select, Implement, Assess, Authorize, Monitor and Preparation framework. The goal is to continually reassess and measure the effectiveness of control implementation and feed that back into the work cycle.

Definitions

The following terms are used during the risk management process and procedure:

1. Vulnerability – A weakness or configuration that can be exploited by an adversary or threat actor to compromise the confidentiality, integrity, or availability of university computer systems.
2. Threat – The attack type actor and or attack vector. These range from internal misconfiguration through malicious insider actions to script kiddie, organized crime, and nation state actors.
3. Risk – Calculated simply as the Threat * Vulnerability. It expresses the likelihood and impact.
4. Remediation – The actions taken to block or prevent or detect the risk event early thereby reducing its impact.
5. Control Framework – The definition of controls or measures that the University will put in place to reduce the overall risk to operations.

Roles and Responsibilities

The following are the key responsibilities in the risk management process:

1. CIO, CISO, or Qualified Individual is accountable for:
   - Ownership and improvement of the risk management policy and process
2. Ensuring the execution of the Risk Management process at least annually and on discovery of significant new threats, vulnerabilities, or changes in the IT landscape.
   - Definition of the system boundary for which risk management is to be performed.
   - Communicating the overarching risk position at least annually to the Executive team and Management Board and on any significant change.
   - Defining the acceptable level of IT Security Risk for each system or portfolio of systems under guidance from the executive team and board.
3. IT Director – is responsible for:
   - Maintaining the risk register
   - Mitigating threats as agreed as well as
   - Contributing to each risk assessment cycle.
4. IT Team members are responsible for reporting any potential threats and vulnerability to the IT director for inclusion in the risk register.
5. Application and System Owners
   - Identification of risk scenarios for analysis
   - Mitigation planning
   - Remediation of risk findings as agreed during prioritization and reporting.
6. Business and Product Management team
   - Identification of risk scenarios for analysis.
   - Assistance in forecasting risk likelihood and impact for estimation purposes.