RISK ASSESSMENT POLICY

PURPOSE

The purpose of this policy is to facilitate compliance with applicable Federal and State laws and regulations, protect the confidentiality and integrity of IT Resources, and enable informed decisions regarding risk tolerance and acceptance.

SCOPE

This IT policy, and all policies referenced herein, shall apply to all members of the <Org Name> community including, but not limited to affiliates, trainees, volunteers, faculty, students, administrative officials, staff, alumni, authorized guests, delegates, and independent contractors (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, the IT Resources, whether individually controlled, shared, stand-alone, or networked. The titles will be referred collectively hereafter as "<Org Name> Community".

POLICY

General

- <Org Name> must categorize information, services, and systems per Federal laws, Executive Orders, directives, policies, regulations, and standards.
- Security categorization must be documented in a standard location accessible to the personnel responsible for managing the security, service, and system.
- The <Accountable Person's Title> (or designee) is authorized to perform periodic information security risk assessments to determine areas of vulnerability and to initiate appropriate remediation.
- <Org Name> uses formal Information Security Risk Management (ISRM) programs that identify risks and implement plans to address and manage them.
- The <Accountable Person's Title> is responsible for managing the Information Security Risk Management program and coordinating the development and maintenance of program policies, procedures, standards, and reports.
- The ISRM program is based on risk assessment and developed in consideration of organizational priorities, staffing, and budget.
- Risk assessments must identify, quantify, and prioritize risk acceptance and objectives relevant to the organization. The results are to guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls to protect against these risks.
- The risk assessment must include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the calculated risks against risk criteria to determine the significance of the risks (risk evaluation).

- Risk assessments are performed periodically to address changes in security requirements and the risk situation (e.g., threats, vulnerabilities, impacts, risk evaluation, and data classification).
- Risk assessments are to be undertaken systematically, capable of producing comparable and reproducible results. The information security risk assessment should have a clearly defined scope to be effective and should include relationships with risk assessments in other areas, if appropriate.
- Risk assessment results must be reviewed at least annually or when there are significant changes to the operating environment, but are expected to be reviewed as part of relevant upgrades, maintenance, and contract renewals.

THIRD-PARTY ASSESSMENTS

- Vendors, suppliers, and third parties will be grouped into Tiers based upon the criticality of the system or service provided and the type of data involved.
- An inventory will be maintained by <Accountable Person's Title> for each Tier showing the vendor, supplier, or third party and why they are in that tier.
- Standards will be developed to ensure an appropriate risk assessment is performed based upon the Tier to include the frequency of review.

DEFINITIONS

- **Control** is a defined process or procedure to reduce risk.
- **Inherent Risk** is the level of risk before Risk Treatments (controls) are applied.
- **IT Resources** include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
- **Information Security Risk Management (ISRM)** is a program that consistently identifies and tracks information security risks, implements plans for remediation, and guides strategic resource planning.
- **Residual Risk** is a level of risk that remains after Risk Treatments (controls) are applied to a given Risk.
- **Risk** is the possibility of suffering harm or loss or the potential for realizing unwanted negative consequences of an event.
- **Risk Management** is the ongoing management process of assessing risks and implementing plans to address them.

- **Risk Assessment** is the process of taking identified risks and analyzing their potential severity of impact and likelihood of occurrence.
- **Risk Treatment** is the process of managing assessed or identified risks. Risk treatment options are risk avoidance (withdraw from), sharing (transfer), modification (reduce or mitigate) and retention (acceptance).

EXCEPTIONS

Exceptions from certain policy provisions may be sought following the <Org Name> Exception Process.

ENFORCEMENT

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

RELATED DOCUMENTS

- Data Classification
- System Criticality
- Patch Management
- Vulnerability Management

VERSION HISTORY

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0				Document Origination

Appendix A: Definitions