POLICY STATEMENT 122 STANDARD 2
RISK MANAGEMENT

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: December 12, 2022
Last Revised: none

I. PURPOSE

As an institution of higher education, Louisiana State University at Eunice ("University" or "LSU Eunice") is charged with maintaining systems and data for administrative and academic purposes. These assets are critical to the mission of the University, and the acceptable use of these systems and data sets mustbe managed with a formalized Information Security Program.

A major element of protecting the University's Information Technology (IT) assets is managing risks that result from vulnerabilities and threats to the confidentiality, integrity, and availability of LSU Eunice data and information systems. Managing risk is primarily accomplished with a formalized Risk Management Program.

The purpose of this standard is to describe risk management standards as they pertain to the LSU Eunice systems.

II. DEFINITIONS

Threat. Threat is a possible danger that might exploit a vulnerability to breach security and therefore cause potential damage or exposure to information systems, data, and/or supporting technology.

Vulnerability. Vulnerability is a weakness which can be exploited by a threat actor, such as a hacker, to perform unauthorized actions on an information system.

III. STANDARDS

A. Risk Management Program

1. The Office of Information Technology (OIT) shall develop a comprehensive risk management program that provides documentation of identified and/or reported risks, which can then be presented to University Administration Officials as necessary.

2. Appropriate processes and procedures must be established to allow for the reporting of risk information.

3. Campus departments and/or units shall communicate all identified security risks to OIT through established processes and procedures.

4. Compliance based risk management programs may be established, as needed, to implement appropriate risk management activities.

B. Risk Assessment

1. When data collection occurs, as part of risk assessment, the collecting entity (e.g., LSU Eunice OIT) shall define the scope and business context of the risk assessment and identify the responsibility of all involved parties.

2. Risk interview survey shall be developed to ensure a comprehensive set of information is being collected related to risk in a consistent manner.

3. Risk assessment practices shall be developed based on an industry standard framework, such as the Educause Risk Management Framework or the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), as well as business practices.

4. Risk assessment processes and procedures shall account for the University environment as well as business processes involved.

5. Risk assessment must not be limited to information systems/services, but also include business processes, data flows, physical security, and other components relevant to protect confidentiality, integrity, and availability of data.

C. Risk Analysis

1. OIT must develop a risk register which must be utilized to identify, analyze, and document risks.

2. A University risk register document should aggregate risks from other risk registers, e.g., departmental risk register, compliance-based risk register, etc.

3. The University risk register shall be maintained by OIT and include, at minimum, the following attributes:

a. Risk identification date

b. Risk status (i.e., the extent that the risk has been addressed)

c. Risk statement

d. Risk owner

e. Risk probability (i.e., likelihood of the risk being realized)

f. Risk impact of the risk should it be realized

g. Risk priority based on likelihood and impact

h. Risk mitigation plans

D. Risk Mitigation

1. Risk mitigation plans shall be formulated and documented leveraging one of the following strategies:

    a. Acceptance – accepting the risk and its associated impact as cost of conducting business.

    b. Avoidance – ceasing to perform the activity that results in the documented risk

    c. Transfer – contractually shifting risk from one party to another (e.g., outsourcing)

E. Mitigate – taking corrective actions to reduce the likelihood and/or impact of the risk.

1. Risk mitigation plans must be documented in the risk register at the appropriate level where it was identified, i.e., unit, department, and/or the University.

2. A risk acceptance form, developed by OIT, must be completed by all relevant parties identified in the form. The acceptance form must be submitted to OIT for documentation and record retention purposes.

IV. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	04/20/2022	Initial Draft	OIT