POLICY STATEMENT 120
INFORMATION SECURITY PROGRAM

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: October 17, 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 security of these systems and data sets must be managed with a formalized Information Security Program.

The purpose of this policy is to identify requirements to establish a comprehensive Information Security Program at LSU Eunice.

II. DEFINITIONS

Action Review. Action review refers to a managerial review function over a particular business process to ensure that proper segregation of duties is occurring.

Approval/Authorization. Approval/Authorization refers to the formalized approval of a transaction that allows it to complete.

Asset. A resource, process, product, information infrastructure, etc. whose loss or compromise could intangibly affect its integrity, availability, or confidentiality, or it could have a tangible dollar value. The loss or compromise of an asset could also affect an entity's ability to continue business. Examples of assets including, but are not limited to,equipment, software, algorithms, and data.

Asset processing. Asset processing is the act of fulfilling the transaction (e.g., granting system/data level access, account reimbursement) as well as creating and maintain the records of the transaction.

Information Security Program. The collection of administrative, physical, and technical safeguards implemented to mitigate the risks to the integrity, availability, and confidentiality of information technology assets.

Initiation. Process initiation is the responsibility of setting a process in motion (e.g., creating/submitting/initiating forms, requests, etc.)

Responsibility. The job functions and associated activities performed in a particular operation or process as a function of a role.

Role. A defined position assumed by employees at an entity.

Segregation of Duties. Segregation of Duties (SOD) is the act of dividing duties and responsibility among various individuals to reduce the possibility of unauthorized, unethical, illegal, or unintentional modification or misuse of information system resources.

Standard. Standards are defined actions and/or rules that provide support and direction for compliance with policies.

III. POLICY STATEMENT

A. Roles and Responsibilities

1. LSU Eunice must define roles and responsibilities related to Information Security Program, including but not limited to:

    a. University Administration Officials

    b. Department Head of Information Technology

    c. Information Security Analyst

    d. Data Analyst

    e. Information Security Team

    f. IT Security Analyst

    g. Departmental Technology Support Professionals

    h. Data Functional Owner

    i. Data Steward

    j. Data Custodian

    k. Data Consumer

2. Individuals assigned roles associated with Information Security Program may delegate tasks but must remain accountable for all systems and data within their purview.

B. Segregation of Duties

1. LSU Eunice must segregate duties and areas of responsibility for any processes or actions that affect campus information technology assets, including, but not limited to:

    a. Process/action development/initiation

    b. Process/action approval

c. Asset processing

d. Process/action review/reconciliation

C. Security Awareness

1. LSU Eunice must specify security awareness training requirements for all users of information technology and data, as well as the associated completion timelines and recurrence schedules.

2. LSU Eunice must outline all security awareness training programs available,the intended audience, and the mechanisms for communication and training delivery.

3. LSU Eunice must maintain records related to completion of applicable trainings.

D. Policy Management

1. LSU Eunice must specify a nomenclature and standard format for all Policies and Standards associated with Information Security Program.

2. LSU Eunice must outline maintenance procedures, including review workflows and schedules related to policies and standards.

IV. STANDARDS

A. The defined roles and respective responsibilities are outlined in Standard LSU Eunice-ST-120-1.

B. Controls necessary for SOD are outlined in Standard LSU Eunice-ST-120-2.

C. Details related to Security Awareness trainings are outlined in Standard LSU Eunice-ST-120-3

D. Policies and Standards review information is outlined in Standard LSU Eunice-ST-120-4

V. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	2/25/2022	Initial Draft	OIT