POLICY STATEMENT 120
INFORMATION SECURITY PROGRAM

Monitoring Unit: Information Technology Services
Initially Issued: July 21, 2023

PURPOSE

As an institution of higher education, the Louisiana State University A&M Baton Rouge Campus ("University" or "LSUAM") is charged with maintaining systems and data for administrative, academic, and research 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 LSUAM.

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 be completed.

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 include, 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 maintaining 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.

Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident Response – The process through which an entity addresses an incident, cyber-attack and/or a breach.

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

IT Asset – For the purpose of these policies, IT Asset is a subset of Asset and specifically refers to hardware that have compute and storage capabilities (e.g., laptops, desktops, servers/virtual servers, mobile devices, etc.) and is utilized to store, process, access, and/or handle Data.

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.

POLICY STATEMENT

A. Roles and Responsibilities
    1. LSUAM must define roles and responsibilities related to the Information Security Program, including but not limited to:
        a. University Administration Officials
        b. Chief Information Officer
        c. Chief Information Security Officer
        d. Chief Data Officer
        e. Information Security Team
        f. IT Security Analyst
        g. Departmental Technology Support Professionals
        h. Data Functional Owner (e.g., Registrar for student data, faculty member for respective research data, Chief Human Resource Officer for HR data, etc.)
        i. Data Steward (e.g., Registrar for student data, faculty member for respective research data, Director of Financial Aid for Financial Aid data, etc.)
        j. Data Custodian (e.g., departmental technology support professionals for departmental data, faculty member for respective research data, etc.)
        k. Data Consumer

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

B. Segregation of Duties
    1. LSUAM must segregate duties and areas of responsibility for any processes or actions that affect 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. LSUAM 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. LSUAM must outline all security awareness training programs available, the intended audience, and the mechanisms for communication and training delivery.
    3. LSUAM must maintain records related to completion of applicable trainings.

D. Policy Management
    1. LSUAM must specify a nomenclature and standard format for all Policies and Standards associated with Information Security Program.
    2. LSUAM must outline maintenance procedures, including reviewing workflows and schedules related to policies and standards.
    3. LSUAM must define an exceptions process for all policies and standards including appeals process for exceptions that are denied.

E. Policy and Standard Non-compliance
    1. Non-compliance with any IT Security policies and standards may result in blocking of network access of IT asset(s) and/or users(s) until the identified issue(s) has been resolved in collaboration with appropriate support personnel and/or user, where applicable.

STANDARDS

A. The defined roles and respective responsibilities are outlined in Standard PS-120-ST-1.
B. Controls necessary for SOD are outlined in Standard PS-120-ST-2.
C. Details related to Security Awareness trainings are outlined in Standard PS-120-ST-3.
D. Policies and Standards review information is outlined in Standard PS-120-ST-4.

REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	7/21/2023	Initial Draft	Information Technology Services