POLICY STATEMENT 133
INFORMATION TECHNOLOGY AND SECURITY OPERATONS

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: June 20, 2023
Last Revised: none

I. PURPOSE

As an institution of higher education, the Louisiana State University at Eunice Campus (“University” or “LSU Eunice”) is charged with maintaining systems and data for administrative, academic, and research purposes. Information Technology (IT) and Security Operations play a critical role in managing the security posture, and thus must be managed with a formalized IT and Security Operations Policy.

The purpose of this policy is to define the required processes and activities pertaining to IT and Security Operations.

II. DEFINITIONS

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 LSUE’s ability to continue business.

Backup. A copy of files and programs made to facilitate recovery if necessary.

Change Management. A process designed to understand and minimize risks while making IT changes.

Enterprise Architecture. The description of an enterprise’s entire set of information systems: how they are configured, how they are integrated, how they interface with the external environment at the enterprise’s boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise’s overall security posture.

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.

Incident Response Plan. The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit the consequences of a malicious cyber- attack against an organization’s information system(s).

Information Technology Asset. For the purpose of these policies, IT Asset is a subset of Asset and specifically refers to hardware (laptops, desktops, servers/virtual servers, external storage devices, mobile devices, etc.) utilized to store, process, access, and/or handle Data.

Patch. A repair job for a piece of programming; also known as a fix. A patch is the immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's website.

Threat. Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification, or information, and/or denial of service. Threats can also cause information systems to become unavailable.

Vulnerability. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Management. A process to identify vulnerabilities on assets that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.

III. POLICY STATEMENT

A. Threat Management

1. LSU Eunice shall establish processes and procedures for threat management.

2. LSU Eunice shall identify, document, and, where applicable, procure services that provide threat feeds and/or information.

B. Incident Response

1. LSU Eunice shall define incident categories and reporting mechanisms.

2. LSU Eunice shall define, implement, and communicate the institution's Incident Response Plan.

C. Change Management

1. LSU Eunice shall establish processes and procedures for change management.

2. LSU Eunice shall identify and document IT assets in scope of change management.

D. Enterprise Architecture

1. LSU Eunice shall develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations, assets, and individuals.

E. Backup Management

1. LSU Eunice shall define backup requirements for critical systems.

2. LSU Eunice shall develop processes and procedures for backup management and recovery.

F. Patch Management

1. LSU Eunice shall establish a patch management program to implement patches and system updates.

G. Vulnerability Management

1. LSU Eunice shall establish a comprehensive vulnerability management program.

2. LSU Eunice shall identify, procure, and implement appropriate tools and technologies to support vulnerability management programs.

H. Security Metrics and Reporting

1. LSU Eunice shall establish information security reporting requirements, metrics, and timelines to monitor effectiveness of the Information Security Program.

IV. STANDARDS

A. The Threat Management standards are outlined in LSU Eunice Policy Statement 133 Standard 1.

B. The Incident Response standards are outlined in LSU Eunice Policy Statement 133 Standard 2.

C. The Change Management standards are outlined in LSU Eunice Policy Statement 133 Standard 3.

D. The Enterprise Architecture are outlined in LSU Eunice Policy Statement 133 Standard 4.

E. The Backup Management standards are outlined in LSU Eunice Policy Statement ST 133 Standard 5.

F. The Patch Management standards are outlined in LSU Eunice Policy Statement 133 Standard 6.

G. The Vulnerability Management standards are outlined in LSU Eunice Policy Statement 133 Standard 7.

H. The Security Metrics and Reporting standards are outlined in LSU Eunice Policy Statement 133 Standard 8.

V. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	03/05/2023	Initial Draft	Office of Information Technology