POLICY STATEMENT 120 STANDARD 4
POLICY MANAGEMENT

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 datasets must be managed with a formalized Information Security Program.

The purpose of this standard is to describe the required components of policy management as it relates to the Information Security Program at LSU Eunice.

II. DEFINITIONS

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

III. STANDARDS

A. The Office of Information Technology (OIT) must develop and maintain information security policies and standards.

B. All policy documents must be reviewed on an annual basis.

C. All standard documents must be reviewed on an annual basis, at minimum, or when a significant change occurs within the University technology environment which would impact the security posture of the University.

D. Policies and standards must also be reviewed and revised, as needed, when changes to legal, regulatory, and/or contractual requirements change.

E. All policies must follow University processes of policy review and approval processes.

F. Any request for a policy and/or standard exception must be submitted to OIT.

1. All exceptions must be evaluated by OIT, in conjunction with the submitter and relevant stakeholders, to determine information security risk. The evaluation must be formally documented and agreed upon by all stakeholders.

2. The exception requests would then be submitted for approval through University processes of policy review and approval.

3. A master document must be maintained for all exceptions.

4. All exception requests must be evaluated on an annual basis, at minimum, unless exempted from the process by the exception approval process.

G. The minimum requirements for documented policies and their related standards, as it relates to OIT, are as below, but are subject to change:

Policy Reference	Policy	Standard Reference	Standards
PS-120	Security Program	PS-120-ST-1	Roles and Responsibilities
		PS-120-ST-2	Segregation of Duties
		PS-120-ST-3	Security Awareness
		PS-120-ST-4	Policy Management
PS-121	Acceptable Use	PS-121-ST-1	Acceptable Use - Network
		PS-121-ST-2	Acceptable Use - Systems
		PS-121-ST-3	Acceptable Use - Applications
PS-122	IT Risk Management	PS-122-ST-1	Internal and External Security Assessment
		PS-122-ST-2	Risk Management (DR/BCP, third party risk, risk register, periodic reviews, etc.)
PS-123	Personnel	PS-123-ST-1	Security responsibilities in Job Descriptions
		PS-123-ST-2	Employee lifecycle (Background checks, hiring, terminations, etc.)
PS-124	Data Management	PS-124-ST-1	Data classification (linked to asset classification)
		PS-124-ST-2	Data handling/processing
		PS-124-ST-3	Data storage (encryption, data masking, data scrambling, etc.)
		PS-124-ST-4	Data privacy
PS-125	Asset Management	PS-125-ST-1	Asset Classification (based on Data Classification)
		PS-125-ST-2	Configuration Management
		PS-125-ST-3	Inventory Management
		PS-125-ST-4	Asset Provisioning and Deprovisioning
PS-126	Encryption	PS-126-ST-1	Encryption and Key Management
PS-127	Compliance	PS-127-ST-1	Contract Management (Data Processing Agreement, BAA, Data protection security language, etc.)
		PS-127-ST-2	Compliance Programs (including Reporting and Training)
		PS-127-ST-3	Login Banners, disclaimers, and consents
PS-128	Identity and Access Management	PS-128-ST-1	Identity Management (Lifecycle, Unique Identifier, provisioning, deprovisioning, etc.)
		PS-128-ST-2	Account Management (Lifecycle, provisioning, deprovisioning, etc.)
		PS-128-ST-3	Authentication (MFA, SSO, Password Management, etc.)
		PS-128-ST-4	Authorization (Least Privilege, Privileged Access, access reviews, access recertifications, etc.)
PS-129	Physical Security	PS-129-ST-1	Surveillance Camera
		PS-129-ST-2	Physical Access Controls (Biometrics, card access, etc.)
		PS-129-ST-3	Fire Protection
		PS-129-ST-4	Critical and Sensitive areas
		PS-129-ST-5	Facility Planning
PS-130	Application Security	PS-130-ST-1	Secure application development
		PS-130-ST-2	Application Security Review (Code review, configuration review, etc.)
		PS-130-ST-3	Cloud application management
PS-131	Network Security	PS-131-ST-1	Network Architecture (Zones - Trusted and Untrusted, NAC, etc.)
		PS-131-ST-2	Network Firewall devices and appliances
		PS-131-ST-3	IDS/IPS
		PS-131-ST-4	Remote access (VPN, RDP Gateway, etc.)
		PS-131-ST-5	Wireless
		PS-131-ST-6	Cloud based network
PS-132	System Security	PS-132-ST-1	AV/Malware
		PS-132-ST-2	Host based network protection (firewall, intrusion prevention/detection, etc.)
		PS-132-ST-3	Removable media
		PS-132-ST-4	Physical media
		PS-132-ST-5	File integrity monitoring
		PS-132-ST-6	Mobile Device Management and Bring Your Own Device
		PS-132-ST-7	Endpoint Application Management (end-user software)
		PS-132-ST-8	Operating System Management (laptops, desktops, Servers)
		PS-132-ST-9	Web Application Management (IIS, Apache, middleware, etc.)
		PS-132-ST-10	Database (SQL, MySQL, Hadoop, etc.)
PS-133	Operations	PS-133-ST-1	Threat management
		PS-133-ST-2	Incident response (log collection, review, correlation, documentation, etc.)
		PS-133-ST-3	Change management
		PS-133-ST-4	Enterprise architecture (Dev, Test, Production systems, Cloud infrastructure)
		PS-133-ST-5	Backup management
		PS-133-ST-6	Patch management
		PS-133-ST-7	Vulnerability management
		PS-133-ST-8	Security Metrics and Reporting

IV. REVISION HISTORY

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