PERMANENT MEMORANDUM 36
INFORMATION SECURITY

Monitoring Unit: Office of Information Technology Services
Initially Issued: April 19, 2005
Last Revised: August 4, 2021

I. Introduction and Scope

Louisiana State University (LSU) is committed to protecting the data that is critical to teaching, research, business operations, and the communities that it supports, including data regarding students, faculty, staff, and the public.

To ensure that the data entrusted to LSU is protected from unauthorized use and disclosure, as required by laws, regulations, contractual obligations, and/or business needs, LSU implemented its information security plan in 2005. The latest version of the policy takes into consideration industry best practices for information security as well as Information Security Standards such as NIST 800-53, ISO 27002, and NIST 800-34, among others.

This policy, and the duties and responsibilities provided in it, are applicable to all entities under the auspices of the Board of Supervisors of Louisiana State University, including external affiliates during their association with LSU.

II. Purpose

The purpose of this policy is:

- To ensure the integrity, availability, and confidentiality of LSU data and systems,
- to protect against any anticipated threats or hazards to the integrity, availability, and confidentiality of LSU data and systems, and

In order to ensure that each institution's information security program is reasonably designed and addresses critical Information Security segments, certain minimum requirements are set forth in the following sections.

Section A – Information Security Program and Responsibilities

Section B – Asset Management

Section C – Personnel Management and Training

Section D – Access Control

Section E – Physical and Environmental Security

Section F – Operations Security

Section G – Cryptography

Section H – Communications Security

Section I – System Acquisition, Development, and Maintenance

Section J – Supplier Relationships

Section K – Information Security Incident Management

Section L – Disaster Recovery and Business Continuity Planning

Section M – Compliance

Section N – Compensating Controls

IV. Policy Review Requirements

PM-36, and its sections, will be reviewed and, if necessary, revised by the appropriate body identified by the EITGC:

- If a concern is raised and vetted through the EITGC
- If a change in legislation occurs, or
- Every three [3] years since last approval

V. Glossary

maintained by a User is also subject to this Policy, even if the data is created and/or stored on the User's own personal computer, smartphone, or other personal device.

Disaster: A sudden, unplanned, calamitous event that produces great damage or loss or any event that creates an inability of the institution to provide critical business functions for undetermined period.

Disclosure: the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

Effectiveness: the extent to which planned activities are realized and planned results achieved

Electronic Messaging: Interpersonal messaging through electronic means, such as, e-mail, text messages, instant messaging, etc.

Encryption: The process of transforming plaintext into ciphertext using a cryptographic algorithm and key.

Enterprise: also referred to as "University," refers to the collection of institutions, academic programs, facilities, and other assets governed by the Board of Supervisors of Louisiana State University as defined by the Bylaws and Regulations of the Board of Supervisors. In PMP UonfalnPeened byd ther-9.9 (o)0.( )-8.9 th Ef 1.6 (,")-19.4 (

Information Processing Facilities: any information processing system, service or infrastructure, or the physical location housing it, e.g., machine room, data center, etc.

Integr ity: property of accuracy and completeness

Likelihood: chance of something happening

Malware : (Short for MALicious softWARE) any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses; also, spyware and programming that gathers information about a computer user or takes actions on a computer system without the user's permission.

Management System: set of interrelated or interacting elements of an organization

Outsource: make an arrangement where an external organization performs part of an organization's function or process; external organization is outside the scope of the management system, although the outsourced function or process is within the scope.

Performance: measurable result; can relate either to quantitative or qualitative findings; can relate to the management of activities, processes, products (including services), systems or organizations.

Physical Safeguards: security measures and/or mechanisms implemented to provide physical security to a defined area and/or location; also referred to as "Physical Security Controls."

Policy: intentions and direction of an organization as formally expressed by its authorized management

Process: set of interrelated or interacting amono9 (awCTc 0 Tw 128.9 (to))Tj EMC /P <</MCID

Review: activity undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve established objectives

Risk: effect of uncertainty on objectives, an effect of which is a deviation from the expected — positive or negative; often characterized by reference to potential events and consequences, or a combination of these. It is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence; in the context of information security management systems, can be expressed as effect of uncertainty on information security objectives; associated with the potential that threats will exploit vulnerabilities of an information asset or group of incy,gro7.4 ( )-.6 (es00.6 (gr)-

Technical Safeguard: hardware, software, and/or firmware mechanisms implemented and/or executed to provide automated protection to a system or application; also referred to as “Technical Controls.”

Threat: potential cause of an unwanted incident, which may result in harm to a

Section A - Information Security Program and Responsibilities

1. Requirement A1 – Information Security Program

Each LSU institution shall develop, implement, and maintain a comprehensive information security program that addresses, administrative, technical, and physical controls which are appropriate to the size, complexity, nature, and scope of the activities of the institution and the sensitivity of the data. This institution information security program shall be designed, at a minimum, to align with all requirements included within PM-36.

2. Requirement A2 - Information Security Program Responsibilities

The LSU Executive Information Technology Governance Council (EITGC) is responsible for approving security strategies that support an Enterprise Information Security Program, as well as providing oversight for each institution's information security program.

Each LSU institution shall define IT security responsibilities to ensure that the requirements of this Memorandum are fulfilled. Individuals with assigned information security responsibilities may delegate security tasks to others; however, shall remain accountable and ensure delegated tasks have been correctly performed. In particular, each institution's management must identify, define, and document roles responsible for the following:

- Overall information security program
- All IT *assets*
- Information security processes, including Information Security Incidents
- Access management
- Information security aspects of supplier relationships

3. Requirement A3 – Risk Management Process

Each LSU institution shall develop a risk management process that:

- Identifies reasonably foreseeable internal and external *risks* to the *integrity*, *availability,* and *confidentiality* of LSU *data* and systems that could result in the unauthorized *disclosure*, misuse, alteration, destruction, or other compromise of such *data* and systems, and assess the sufficiency of any safeguards in place to control these *risks.*
- Design and implement safeguards to mitigate the *risks* identified through the institutional *risk assessment*, and regularly test or otherwise monitor the *effectiveness* of the safeguards/*controls*, systems, and procedures.

4. Requirement A4 – Segregation of Duties

Each LSU institution shall segregate duties and areas of responsibility to ensure that any processes or actions that affect assets shall require a minimum of two individuals to execute, to prevent unauthorized or unintentional modification or misuse of institution's assets. These duties and areas of responsibility include but are not limited to:

- x Process/Action Development/Initiation
- x Process/Action Approval
- x Asset Processing
- x Process/Action Review/Reconciliation

Any combination of responsibilities into a single position which results in the incumbent being required to approve their own work, or otherwise creates a conflict of interest, is prohibited.

5. Requirement A5 –

Each LSU institution shall develop and implement written policies and procedures to ensure that all LSU institution property previously assigned to a departing individual is returned.

All faculty, staff, students, and *external affiliates* shall ensure that any LSU institutional *asset* stored or otherwise contained on personal *assets* are permanently removed upon termination of their employment, contract, enrollment, agreement, or at the end of a predefined period after separation as defined in the institute's *policy*.

6. Requirement B6 – Data Governance and Classification

Each LSU institution shall establish a framework for *data* governance which provides consistent, repeatable, and sustainable *processes* for the management of *data*, that reduces inefficiencies, promotes good stewardship of resources, and reduces *risk* to the LSU community. Additionally, as part of *data* governance, each LSU institution shall classify *data* according to the impact of loss of *integrity*, *availability,* and/or *confidentiality*. At a minimum, the institution's classification shall consist of three categories: public, protected, or *restricted data*.

7. Requirement B7 – Labeling of Data

Each LSU institution shall develop and maintain an appropriate set of procedures for *data* labeling in accordance with the *data* classification scheme adopted by the institution. Labeling may take one of two forms:

- Explicit Labeling – Each *asset* containing *data* shall receive an explicit label describing the classification of that *data* as determined in Requirement B1 whenever the *data* is removed from institution's designated secure areas.
- Characteristic Labeling – Each classification shall be described in terms of its characteristics and *attributes*. Any *data* meeting those characteristics and *attributes*

9. Requirement B9 – Management of Removable Media

Each LSU institution shall implement written procedures for the management of *removable media* in accordance with the *data* classification scheme adopted by the institution.

10. Requirement B10 – Disposal of Assets and Media

Disposal of *assets* shall not occur unless the disposal is authorized by the appropriate official of the institution. Each LSU institution shall follow all applicable state policies on the disposal of *assets* and implement written procedures to securely dispose of media when no longer required in accordance with applicable state policies and the procedures developed for handling of *assets* subject to the *data* classification scheme adopted by the institution.

11. Requirement B11 – Risk Management Program

Each LSU institution shall implement a written *information security risk management* program to manage the potential *risks* and *vulnerabilities* to the

Each LSU institution shall implement appropriate written *policies*, *processes*, and procedures to perform background *verification* checks on selected candidates for employment commensurate with their roles, responsibilities, and the assets to be accessed. Repeat background *verification* checks shall be conducted for employees, based upon the institution's *risk assessment,* or based on their roles and responsibilities.

2. Requirement C2 – Termination of Employment, Enrollment or Affiliation

Each LSU institution shall develop written policies and procedures to ensure that all terminations of employment, enrollment or affiliation are recorded, and notification provided to all necessary departments.

3. Requirement C3 – Information Security Training

Each LSU institution shall develop written policies and procedures to require individuals with access to *information system assets* to complete *information security* training appropriate for their role and responsibilities at the institution. If the individual's role or responsibilities change, then the individual's training *requirements* shall be reassessed and new training shall occur, if required. *Information security* training can be provided by any appropriate method including but not limited to classroom-based, distance learning, web-based, and self-paced.

4. Requirement C4 – Training Records

Each LSU institution shall maintain records of all *information security* training provided for a period required by applicable laws, regulations, and/or policies.

E. Requirement D3.5 – Generic IDs
When operational necessity requires *generic IDs*, each institution shall develop written procedures and *controls* to prevent abuse.

4. Requirement D4 – Management of User Authentication Information

Provisioning and disbursement of logon credentials, such as passwords, pins, and tokens, shall be controlled through a documented procedure to ensure that the *data* remains confidential and secure.

5. Requirement D5 – Provisional Access

Each LSU institution shall implement procedures to address provisional access under extenuating circumstances.

6. Requirement D6 - Accountability

All *users*

Each LSU institution shall implement a written procedure to ensure the *integrity* of application environments. *Access controls* must be implemented, as appropriate, for all application environments, such as development, test, and production. All changes to systems, source code, and program libraries shall be properly documented, authorized, and tested before moving to the production environment.

11. Requirement D11 – Working Remotely

Each LSU institution that permits working remotely shall implement reasonable *administrative* and *technical safeguards* to protect *assets* based on the *risks* identified in each institution's *risk assessment*.

Section E - Physical and Environmental Security

1. Requirement E1 – Facilities Requirements Planning

Each LSU institution shall develop and implement written policies and procedures for developing *requirements* to ensure the *reliability* and physical security of the *information processing facilities*.

2. Requirement E2 – Emergency Procedures

Each LSU institution shall develop and implement written procedures to address emergency situations that could potentially threaten the physical security of *information processing facilities*.

3. Requirement E3 – Physical Security Perimeter

Each LSU institution shall define a physical security perimeter which contains all essential and/or sensitive physical elements of *information processing facilities*, including off-site locations, based on its IT *risk assessment*.

4. Requirement E4 – Physical Security Perimeter Safeguards

Each LSU institution shall develop and implement safeguards to ensure the *integrity*, *availability*, and *confidentiality* of the area contained by the physical security perimeter.

5. Requirement E5 – Critical Information System Protection

Each LSU institution shall locate and protect critical *information systems*, as identified by institution's *risk assessment*, in a manner that minimizes the *risk* of service interruption and/or *information system* compromise resulting from potential environmental *threats*, hazards, or opportunities for unauthorized access.

6. Requirement E6 – Supporting Utilities

Each LSU institution shall implement reasonable and appropriate *controls* to prevent service interruptions and/or compromises to critical *information systems*

9. Requirement E9 – Delivery and Removal of Assets

Each LSU institution shall implement policies and procedures which require tracking and documentation of equipment brought into and removed from the physical security perimeter as defined in Requirement E3.

10. Requirement E10 – Clear Desk and Clear Screen Policy

Each LSU institution shall implement a written *clear desk policy* and a *clear screen policy* that secures protected and *restricted data* in the form of paperwork, portable storage media, and active computer sessions from compromise.

Section F – Operations Security

1. Requirement F1 – Change Management

7.

Section H – Communications Security

1. Requirement H1 – Network Controls

Each LSU institution shall ensure that the institution's network communications are managed and controlled to protect *data* in *Information Systems*. Each LSU institution shall implement appropriate *physical*, *administrative,* and *technical safeguards* to ensure the security of *data* in networks and the protection from unauthorized access based upon the institution's IT *risk assessment*.

2. Requirement H2 – Security of Network Services

x Security mechanisms and management requirements shall be included in network services agreements for network services that are outsourced. The

ths( )0.60 Tc 0 Tw 4.>Tj0.93s67 a

- Ensure that the systems that collectively provide name/address resolution service (DNS) for the institution are fault-tolerant and implement internal/external role separation.

3. Requirement H3 - Data Transfer Policies and Procedures

Each LSU institution shall have formal transfer policies, procedures, and *controls* in place to protect the electronic transfer of *data*.

4. Requirement H4 – Agreements on Data Transfer

For each LSU institution, agreements shall address the secure transfer of business *data* between the institution and *external affiliates*.

Where agreements on *data* transfer may not be appropriate (e.g., *data* transfers required by law), each LSU institution shall take all reasonable and appropriate steps to ensure that appropriate *controls* are in place for such transfers.

5. Requirement H5 - Electronic Messaging

Each LSU institution shall establish standards to appropriately protect *data* exchanged via *electronic messaging* based on each institution's *risk assessment*.

6. Requirement H6 - Confidentiality or Non-disclosure Agreements

Each LSU institution shall develop agreements for *confidentiality* or non-*disclosure* reflecting each institution's needs for the protection of *data* based on the institution's *risk assessment*.

Section I – System Acquisition, Development, and Maintenance

1. Requirement I1 – Information Security Requirements

Each LSU institution shall establish *information security requirements* in compliance with this Memorandum for both new *information systems* and enhancements to

systems developed and/or enhanced within the institution. The Secure Development *Policy* must also be shared and adopted by any *external affiliate* when development is *outsourced* in accordance with Requirement I10.

7. Requirement I7 – Production Platform Changes

Each LSU institution shall have a procedure for evaluating automated updates and the application of upgrades, system patches, service packs, fix packs, and hot fixes which may impact the *performance* of the production environment.

8. Requirement I8 – Secure System Engineering Principles

Each LSU institution shall develop principles for engineering systems securely which are documented, *reviewed* on a regular basis, and applied to any *information system* implementation.

9. Requirement I9 – Configuration Management

Each LSU institution shall develop written *policies* and procedures to identify, track, and determine the appropriate values of configuration items of devices, hardware, and software that comprise the institution's *IT infrastructure*.

10. Requirement I10 – Outsourced Development

Each LSU institution shall develop *processes* and procedures for *monitoring* any development *outsourced* to a third-party.

11. Requirement I11 – Information System Security Testing

Each LSU institution shall implement testing procedures for security *controls* throughout the *information system* lifecycle.

12. Requirement I12 – Information System Acceptance Testing

Each LSU institution shall have procedures for acceptance testing throughout the *information system* lifecycle.

13. Requirement I13 – Data Used for Testing and Training

Each LSU institution shall ensure that test *data* resembles production system *data* to extent necessary to facilitate accurate testing.

14. Requirement I14 – De-Identification of Test and Training Data

Where feasible, each LSU institution shall implement *processes* to remove, mask or modify any identifiers contained within protected or *restricted data* when such *data* is *used* for testing and training purposes. If not feasible or if *data* containing protected or *restricted data* is required for testing purposes, the same protections shall be *used* for the test *data* as are in place for production *data*.

15. Requirement I15 – Access to Testing Environments

Each LSU institution shall ensure that access to the test environment is limited only to those individuals performing tests on the application or system.

Section J – Supplier Relationships

1. Requirement J1 – Information Security Policy for Supplier Relationships

Each LSU institution shall develop *information security requirements* for mitigating the *risks* associated with *suppliers*' access to the institution's *assets*, based on the respective institution's *risk assessments*. These *information security requirements* shall be established and agreed upon in writing with each *supplier*

Section K – Information Security Incident Management

1. Requirement K1 – Incident Response Plan

Each LSU institution shall develop a written incident response plan that:

- Provides the LSU institution with a roadmap for implementing its incident response capability
- Describes the internal capabilities and external needs of incident response
- Provides a high-level approach for how the incident response capability fits into the overall LSU institution's operations
- Meets the unique *requirements* of the LSU institution, which relate to mission, size, structure, and functions
- Defines incidents reportable to and by Information Security
- Defines third-party engagement based on incident level and type including, but not limited to, law enforcement, legal counsel, university administration, and strategic communication officers
- Provides metrics for measuring the incident response capability within the LSU institution
- Defines the resources and management support needed to effectively maintain and mature an incident response capability

2. Requirement K2 – Management of Information Security Incidents

Each LSU institution shall develop and implement written *policies* and procedures to detect and report *information security incidents*.

The *Information Security Officer*, or designee, shall assess and classify all *information security incidents* to determine the appropriate course of action.

Each LSU institution shall implement written procedures to respond effectively to *information security incidents*. Each institution must evaluate procedures frequently, at a minimum annually, to ensure all parties involved are aware of their roles and responsibilities.

Each LSU institution shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence in compliance with applicable laws and regulations.

Each LSU institution shall implement written procedures to conduct a post incident analysis and develop recommendations for corrective actions to prevent any recurrence.

Each LSU institution shall maintain documentation of each *information security incident* in accordance with applicable laws and regulations.

Section L – Disaster Recovery and Business Continuity Planning

1. Requirement L1 – Development of a Written Disaster Recovery and Business Continuity Plan

Each LSU institution shall develop a written Disaster Recovery and Business Continuity Plan based on the institution's IT *risk assessment* to effectively respond to and recover from a *disaster*. The Disaster Recovery and Business Continuity Plan shall consider *information security requirements* and include, at minimum, the following:

- Scope of the Plan
- Roles and Responsibilities
- Business Impact Analysis
- Prioritization of Business Functions; including *Recovery Time Objectives* (RTO) and *Recovery Point Objectives* (RPO)
- Command, Control, and Communications *Processes*
- Capacity of IT Resources
- Business Continuity *Process*
- Recovery *Process*

The Disaster Recovery and Business Continuity Plan, including business impact

Section M - Compliance

1. Requirement M1 – Identification of Applicable Legislation and Contractual Requirements

Each LSU institution shall identify and document their relevant statutory, regulatory, and contractual *requirements* for *information security* where applicable and the institution's approach to meet these *requirements*.

2. Requirement M2 – Protection of Records

Each LSU institution shall implement reasonable and appropriate *administrative*, *technical*, and *physical safeguards* to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release based upon the institution's *risk assessment* and in accordance with the institution's records retention policy and applicable laws, regulations, and policies.

3. Requirement M3 – Awareness of *Information Security* and related *policies*

Executive Management shall ensure that all employees, students, and *external affiliates*:

- Are properly briefed on their information security roles and responsibilities upon being granted access to protected or restricted data or information systems
- Are provided with information security expectations of their role
-

5. Requirement M5 – Technical Compliance Review

Each LSU institution shall *review* its *technical* and *physical safeguards* to ensure compliance with all relevant *information security policies* and standards:

- When a new information system is implemented,
- When significant modifications are made to existing information system, or
- Every two years since last review

Section N – Compensating Controls

1. Requirement N1 – Applicability of Compensating Controls

Compensating controls may be considered for *PM-36 requirements* when an LSU institution cannot meet a *requirement* explicitly as stated, due to legitimate technical, or documented business constraints.

Compensating controls must sufficiently offset the *risk* that the original *PM-36*