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
- to protect against unauthorized access to or use of LSU data and systems that could result in substantial harm or inconvenience to the public or LSU faculty, staff, or students.

III. Requirements and Procedures

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

Definitions of terms used throughout this policy:

Access Control: to ensure that access to assets is authorized and restricted based on business and security requirements

Administrative Safeguard: an administrative action, policy, and/or procedure, to manage the selection, development, implementation, and maintenance of security measures to protect electronic information and to manage the conduct of the institution's workforce in relation to the protection of that information. This is also referred to as administrative controls."

Asset: a resource, process, product, information infrastructure, etc. whose loss or compromise could intangibly affect its integrity, availability or confidentiality or could have a tangible dollar value. The loss or compromise of an asset could also affect the institution's ability to continue business. Examples of assets include but are not limited to equipment, software, algorithms, and data. This can also be referenced as information asset(s)."

Attribute: property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means

Authentication: provision of assurance that a claimed characteristic of an entity is correct

Authenticity: property that an entity is who/what they/it is claim(s) to be

Availability: property of being accessible and usable upon demand by an authorized entity

Clear Desk: sensitive or confidential information is not present or visible at a desk.

Clear Screen: sensitive or confidential information is not present or visible on a screen.

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Control: measure that is intended to modify risk; may include any process, policy, device, practice, or other actions which modify risk; may not always exert the intended or assumed modifying effect.

Corrective Action: action to eliminate the cause of a nonconformity and to prevent recurrence

Cryptography: the discipline that embodies the principles, means, and methods for the transformation of data to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification

Data: Any information residing on the institution's IT Infrastructure or held on any other IT Infrastructure on behalf of the institution; includes files, documents, messages in any format, including e-mail messages and posts made on any social media site maintained by/for the institution. All institution's data created and/or

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 PM-36 this is signified by upper case "E" in the term "Enterprise." Individual institutions are referred as either "institution" or "enterprise" (signified by lower case "e")

Event: occurrence or change of a particular set of circumstances; can be one or more occurrences and can have several causes and can also consist of something not happening.

Executive Management: for the purpose of this policy, a person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organization. Sometimes called "management" and can include Chief Financial Officers, Chief Information Officers, Provost, Chancellors, and equivalent roles

External Affiliate: An individual who is not a faculty member, staff member or student of an LSU institution, or who is a third-party vendor, contractor, or supplier, but has been granted access to the institution IT infrastructure due to contractual, regulatory, or other reasons.

External Context: external environment in which the organization seeks to achieve its objectives; external context can include the cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environment, whether international, national, regional, or local; key drivers and trends having impact on the objectives of the organization; and relationships with, and perceptions and values of, external stakeholders.

Generic ID: functional and/or service accounts that serve a specific purpose beyond a user's primary account.

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

Information Security: preservation of integrity, availability, and confidentiality of information; can also involve other properties, such as authenticity, accountability, non-repudiation, and reliability.

Information Security Incident: a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Information Security Incident Management: processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents

Information Security Officer: individual designated within the institution or university with the responsibility for development and maintenance of the information security program

Information Security Program: the collection of administrative, physical, and technical safeguards implemented to mitigate the risks to the integrity, availability, and confidentiality of assets identified in the risk assessment

Information Security Risk: the risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems

Information System: applications, services, information technology assets, or other information handling components

Information Technology (IT) Infrastructure: a compilation of products and services that turn data into functional, meaningful, available information. The IT Infrastructure is the network, the communication physical media, the protocols, the associated software/applications/firmware, the hardware devices that provide connectivity (including but not limited to switches, access points, and routers), and all equipment (including, but not limited to, personal computers, laptops, PDAs, and smart phones) attached thereto regardless of ownership or location.

Information Technology-related Risk: the net mission/business impact (probability of occurrence combined with impact) from a particular threat source exploiting, or triggering, a particular information technology vulnerability. IT related risks arise from legal liability or mission/business loss due to:

- unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information,
- non-malicious errors and omissions,
- IT disruptions due to natural or man-made disasters, and
- failure to exercise due care and diligence in the implementation and operation of the IT.

Integrity: 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 to establish policies, objectives and processes to achieve those objectives; can address a single discipline or several disciplines; system elements include the organization's structure, roles and responsibilities, planning, operation, etc.; scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

Media: Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration (LSI) memory chips, or removable media onto which information is recorded, stored, or printed within an information system.

Mobile Device: includes any device that is both portable and capable of collecting, storing, transmitting, or processing electronic data or images; examples include, but are not limited to, laptops, smartphones, and tablets; also includes storage media, such as USB hard drives or memory sticks, SD or CompactFlash cards, and any peripherals connected to a mobile device or computer capable of collecting, storing, transmitting, or processing electronic data.

Monitoring: determining the status of a system, a process, or an activity; to determine the status, there may be a need to check, supervise, or critically observe.

Non-repudiation: ability to prove the occurrence of a claimed event or action and its originating entities

Objective: result to be achieved; can be strategic, tactical, or operational; can relate to different disciplines (e.g., financial, health and safety, and environmental goals) and can apply at different levels (e.g. strategic, organization-wide, project, product, and process); can be expressed in other ways, e.g., as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g., aim, goal, or target). In the context of information security management systems, information security objectives are set by the organization, consistent with the information security policy, to achieve specific results.

Owner: Person or entity with fiduciary responsibility for an asset; should understand the responsibility of maintaining the security of the asset and have approved management responsibility for controlling the whole lifecycle of an asset; should be able to help define the value of the asset; must evaluate the asset to be assured that the asset receives the appropriate level of security.

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 activities which transforms inputs into outputs

Protected Data: Data of such a nature that unauthorized, disclosure, alteration, or destruction of data could result in moderate level of risk to an entity; Examples include, but are not limited to, research data, intellectual property, etc.; by default, should be treated as protected data unless classified as public or restricted data.

Public Data: Data of such a nature that unauthorized disclosure, alteration, or destruction of data would result in little or no risk to an entity; Examples include, but are not limited to, course information, employee names, research publications, etc.

Recovery Time Objective: overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or business processes

Recovery Point Objective: The point in time to which data must be recovered after an outage

Reliability: property of consistent intended behavior and results

Removable Media: Portable data storage medium that can be added to or removed from a computing device or network; examples include, but are not limited to, optical discs, external/removable hard drives, external/removable Solid-State Drives, flash memory devices, etc.

Requirement: need or expectation that is stated, generally implied; or obligatory; "generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied; a specified requirement is one that is stated, for example in documented information.

Residual Risk: risk remaining after risk treatment; can contain unidentified risk; can also be known as "retained risk"

Restricted Data: Data of such a sensitive nature that unauthorized disclosure, alteration, or destruction of data could cause significant risk to an entity; examples include, but are not limited to student records, employee records, health information, payment card data, etc.

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 information assets and thereby cause harm to an organization.

Risk Assessment: overall process of risk identification, risk analysis, and risk evaluation

Risk Identification: process of finding, recognizing, and describing risks; involves the identification of risk sources, events, their causes, and the potential consequences; can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

Risk Management: coordinated activities to direct and control an organization with regards to risk

Risk Treatment: process to modify risk that can involve avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk, taking or increasing risk in order to pursue an opportunity, removing the risk source, changing the likelihood, changing the consequences, sharing the risk with another party or parties (including contracts and risk financing), and retaining the risk by informed choice; treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention", and "risk reduction;" can create new risks or modify existing risks.

Security Implementation Standard: document specifying authorized ways for realizing security

Sponsor: an LSU institution faculty or staff member who is familiar with the functions of the external affiliate(s) that require access to an asset or assets and accepts responsibility for monitoring the access of an external affiliate(s).

Stakeholder: person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Subsidiary Policies: Institution policies required by Permanent Memorandum 36 (this policy); cannot contradict Federal or State laws, the Bylaws and the Regulations of the Board of Supervisors, or any Permanent Memorandum

Supervisor: Individual responsible for the performance of a user.

Supplier: a person or an organization that provides something that is needed, such as a product or service.

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 system or organization

Use: the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

User: Any individual or entity that utilizes an asset; can be an individual, application, information system, network, etc.

User ID: Unique symbol or character string used to identify a specific user before granting access to an asset.

Utility program: Application(s) utilized by IT Administrators to conduct system, application, network, and/or database administration.

Verification: confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Vulnerability: weakness of an asset or control that can be exploited by one or more threats

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:

- Process/Action Development/Initiation
- Process/Action Approval
- Asset Processing
- 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 – Enterprise Information Security Risk Assessment

The Office of Internal Audit must coordinate, facilitate, and/or perform *Enterprise Information Security Risk Assessments* and report findings to individual institutions as well as to EITGC.

6. Requirement A6 – Exceptions

Exceptions to PM-36 must be submitted, in writing, to the appropriate body identified by EITGC.

Section B – Asset Management

1. Requirement B1 – Responsibility for Assets

Each LSU institution shall complete an inventory of institution owned information system assets, as identified by the institution based on risk assessment, located at all sites and/or geographical locations over which the institution exercises control, maintains the inventory over time, and ensures all information asset management systems are in sync. The inventory shall include, but not necessarily be limited to the following information:

- Description of the asset
- Owner of the asset
- Custodian of the asset
- Classification of the asset by ranking the business impact of the asset, defined by the asset owner, in the following areas:
  - Integrity
  - Availability
  - Confidentiality

2. Requirement B2 – Ownership of Assets

Each LSU institution shall implement written policies and procedures to ensure each asset is assigned a custodian(s). The policies and procedures shall include the following responsibilities for asset owner(s):

- Ensure that assets are inventoried
- Ensure that assets are protected as per asset classification
- Ensure appropriate support is in place for the asset
- Periodically review access restrictions and classifications of assets, considering applicable access control policies
- Ensure proper handling when the asset is removed or destroyed

3. Requirement B3 – Support of Assets

Each LSU institution's *assets* shall have the appropriate support services in place to ensure that the institute's business functions are not compromised. Reasonable effort shall be made to resolve issues efficiently and timely.

4. Requirement B4 – Acceptable Use of Assets

Each LSU institution shall implement policies related to acceptable *use* of the institute's *IT infrastructure* and other *assets*.

5. Requirement B5 – Return of Assets

Each LSU institution's faculty, staff, students, and *external affiliates* shall be responsible and accountable to return all *assets* in their possession upon termination of their employment, contract, enrollment, agreement, or at the end of a predefined period after separation as defined in the institution's *policy*.

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* is deemed labeled with that classification.

8. Requirement B8 – Handling of Assets

Each LSU institution shall develop and implement written procedures and standards for handling *assets* in accordance with the *data* classification scheme adopted by the institution. The written procedures and standards shall include:

- Access restrictions that support the protection requirements for each level of classification
- Maintenance of a record of the authorized recipients of the assets
- Protection of temporary or permanent copies of data to a level consistent with the protection of the original data
- Appropriate storage of the IT assets

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 *confidentiality*, *integrity*, and *availability* of the *assets* identified by Requirement B1. The *risk management* program shall include the following elements at a minimum:

- Identification of the *assets* to be protected as determined in accordance with Requirement B6
- A list of *threats* to the *integrity*, *availability,* and *confidentiality* of the *data* to be protected and the *likelihood* of the *threat's* occurrence
- A list of *vulnerabilities* and predisposing conditions, if applicable, that may affect the impact of a *threat* occurrence.
- A list of *controls* designed to mitigate identified *threats*
- *Risk assessment* methodology and frequency
- Determination of acceptable *risk* thresholds in collaboration with *asset owners* and the institution's *executive management*
- A list of *corrective actions* to address *residual risks* that exceed acceptable *risk* thresholds after existing *controls* have been applied

12. Requirement B12 – Review of Risk Management Program

Each LSU institution shall *review* the elements of their *risk management* program whenever a change occurs in the internal or *external contexts* and periodically but no less frequently than every two years.

13. Requirement B13 – Documentation and Retention

Each LSU institution shall maintain documentation of each of the elements of its *risk management* program listed in Requirement B11. Each institution shall retain the documentation on their *risk management* program for a minimum of three years unless laws and/or regulations, applicable to an institution, specify a longer retention period in which case the longer period shall apply.

Section C – Personnel Management and Training

1. Requirement C1 – Background Verification Checks

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.

Section D – Access Control

1. Requirement D1 – Access to LSU Institutional Assets

Each LSU institution shall implement written policies and procedures to ensure that all access to information *assets* is based on the lowest level of privilege needed to perform assigned duties and responsibilities.

Each LSU institution shall implement policies and procedures to govern access management, such as approval, recertification, and revocation. Access management must be reviewed and addressed throughout a *user's* lifecycle including, but not limited to, job/role changes, changes in responsibilities, employment/affiliation termination, etc.

Each LSU institution shall implement policies and procedures to prevent unauthorized access and/or modification to information *assets*.

2. Requirement D2 – Permitted Access Without Identification or Authentication

Any access permitted on an LSU institution's network without identification or *authentication* shall be documented in the institution's written policies and procedures, and appropriate *controls* shall be implemented to ensure the security of the institution's *assets*.

3. Requirement D3 – User Provisioning and De-provisioning

Each LSU institution shall implement written policies and procedures to provision/de-provision *user IDs* based upon a *users'* affiliation status in authoritative records which include, students, staff, faculty, and *external affiliates*.

A. Requirement D3.1 – External Affiliate Safeguards
   Each LSU institution shall implement appropriate *physical*, *technical,* and *administrative safeguards* to ensure that the access granted to an *external affiliate* is the minimum necessary for the *external affiliate*'s roles and responsibilities.

B. Requirement D3.2 – External Affiliate Sponsor
   Each *external affiliate* shall have at least one *sponsor* who is an employee of the LSU institution who is familiar with the roles and responsibilities of the *external affiliate* that necessitate the *external affiliate*'s access to the LSU institution's network.

C. Requirement D3.3 – Sponsor Responsibilities
   The *external affiliate*'s *sponsor* shall act in the role of the *supervisor* for the purposes of this *policy*. Each *external affiliate sponsor* shall notify the *Information Security Officer,* or their designee, of any changes in the roles, responsibilities, and/or status of an *external affiliate* that would necessitate a change in the *external affiliate's* access.

D. Requirement D3.4 – Unique User IDs
   Each *user* shall be assigned a unique *user ID*.

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* of an LSU institution's *IT infrastructure* shall be responsible for all actions taken using their access credentials. Sharing passwords and other access credentials is strictly prohibited.

All LSU institution's faculty, staff, students, and *external affiliates* shall immediately report to the relevant unit responsible for responding to *Information Security Incidents* at their respective institution when they suspect that their access credentials have been compromised.

7. Requirement D7 – Encryption of Credentials

Each LSU institution shall ensure that *authentication* credentials are encrypted in accordance with industry best practices regarding *authentication* protocols.

8. Requirement D8 – Password Management

All LSU *information systems* that *use* passwords as the primary method of *user authentication* shall require that all *user* accounts be password protected with strong passwords. Each LSU institution shall develop and/or adopt standards for strong passwords, that include:

- Password length
- Password change interval
- Password complexity
- Allowable number of unsuccessful login attempts
- Time period of account suspension after exceeding the allowable number of attempts

9. Requirement D9 – Use of Privileged Utility Programs

Each LSU institution shall develop *administrative* and *technical safeguards* to manage access to *utility programs* to prevent unauthorized *use*.

10. Requirement D10 – Access Control to Application Environments

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* due to a failure of supporting utilities.

7. Requirement E7 – Cabling Security

Each LSU institution shall implement reasonable and appropriate *physical security controls* to create and protect a suitable environment for power and telecommunication cables. This environment, which must be compliant with applicable codes, should protect cabling from interference and damage.

8. Requirement E8 – Information Systems Maintenance

Each LSU institution shall implement written equipment maintenance policies and procedures to ensure the continued *availability* and *integrity* of 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

Each LSU institution shall have a written change control *policy* and procedure to track any changes to mission and/or business-critical *enterprise* IT systems, as identified by the institution's *risk assessment*.

2. Requirement F2 – Separation of Development/Testing and Production Environments

Where feasible, each LSU institution shall separate development/testing and production environments for mission or business critical *enterprise* IT systems.

3. Requirement F3 – Anti-malware Software

Each LSU institution shall develop and implement written policies and procedures to protect against and detect *malware*. All institution owned servers, workstations, and *mobile devices* shall run anti-*malware* software (including spyware detection).

4. Requirement F4 – Blocking Malicious Websites

Each LSU institution shall develop and implement procedures to block access to identified malicious websites.

5. Requirement F5 – Information Backup

Each LSU institution shall implement written policies and procedures to back up software and *data* from critical *information systems* and restore *information systems* from backup media. These procedures shall ensure:

- The backup of user-level data contained in the information system
- The backup of system-level data contained in the information system where applicable
- The backup of information system documentation including security-related documentation
- The confidentiality, integrity, and availability of backup data at storage locations
- The recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure

6. Requirement F6 – Event Logging

Each LSU institution shall implement *event* logs for critical *information systems*, which record *user* activities, exceptions, and faults based on the institution's IT *risk assessment*. *Event* logs shall be produced, kept, and *reviewed* for indications of unusual or inappropriate activity.

Logging facilities and log *data* shall be protected against tampering and unauthorized access.

Each LSU institution shall ensure that appropriate individual(s) are notified when *event* log *data* processing fails and that appropriate steps are taken to restore processing of *event* logs as soon as practical.

7. Requirement F7 – Clock Synchronization

Each LSU institution should synchronize the clocks of all information systems and endpoints to reference a Coordinated Universal Time (UTC) source.

8. Requirement F8 – Installation of Software on Critical Information Systems

Based on the institution's IT *risk assessment*, written procedures shall be implemented to control the installation of software on critical *information systems*. Each LSU institution shall implement *controls* to *monitor* and restrict installation of software as necessary to limit the *risk* to the institution.

9. Requirement F9 – Management of Technical Vulnerabilities

Each LSU institution shall have *processes* in place to scan for and evaluate *vulnerabilities* related to *information systems* and implement appropriate *physical*, *technical*, and *administrative safeguards* to address all *risks* associated with the *vulnerability*.

Section G - Cryptography

1. Requirement G1 – Use of Cryptographic Controls

Each LSU institution that employs *encryption* as a *risk mitigation control* shall implement written policies and procedures for cryptographic *controls* based upon the institution's IT *risk assessment*.

2. Requirement G2 – Cryptographic Standards

Each LSU institution that employs *encryption* as a *risk treatment* shall establish cryptographic standards appropriate for the security *objective* (e.g., *confidentiality*, *integrity*, *authenticity, non-repudiation*, *authentication*, etc.) based upon the institution's IT *risk assessment*. At a minimum, cryptographic modules should meet the standards set forth in applicable industry standards unless technical *requirements* prevent it.

3. Requirement G3 – Cryptographic Key Management

Based upon the institution's IT *risk assessment*, each LSU institution that employs *encryption* as a *risk treatment* shall implement written procedures to support the management and security of cryptographic keys through the entire lifecycle for all instances where *encryption* is *used*.

4. Requirement G4 – Regulation of Cryptographic Controls

Each LSU institution shall ensure that cryptographic *controls* are *used* in compliance with all relevant agreements, legislation, and regulations.

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

- Security mechanisms and management requirements shall be included in network services agreements for network services that are outsourced. The ability of the network service provider to manage agreed services in a secure way shall be determined, regularly monitored, and specified in the agreement for services.
- The security arrangements necessary for services, such as security features, service levels, and management requirements, shall be identified and appropriately reflect the security rankings in the institution's risk assessment. Each LSU institution shall require that network service providers implement these physical, administrative, and technical safeguards.
- Each LSU institution's wireless networks that provide access to the institution's assets shall require authentication prior to granting access. Data traversing the institution's wireless networks shall be encrypted in accordance with Section G – Cryptography of this Permanent Memorandum.
- Each LSU institution shall:
  - Monitor and control communications at the external boundary of the network and at key internal boundaries within the network.
  - Implement subnetworks for publicly accessible system components that are separated from internal organizational networks.
  - Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
  - Control remote activation of collaborative computing devices and provide an explicit indication of use to users physically present at the devices.
  - Require a minimum of two individuals to execute a change to prevent unauthorized or unintentional modification or misuse of institution's assets. 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.
  - Provide the means to indicate the security status of Domain Name Services (DNS) child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
  - Be capable of requesting and performing data origin authentication and data integrity verification on the name/address resolution (DNS) responses the system receives from authoritative sources.

- 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 existing systems as part of the system specification.

2. Requirement I2 – Enforcement of Access Policies

Both new and existing *information systems* shall be capable of enforcing access to *information systems* and *assets* in accordance with applicable institutional policies and procedures developed in compliance with Section D – Access Control.

3. Requirement I3 – Cloud Computing and Other External Information System Services

Each LSU institution utilizing cloud computing services and other external *information system* services shall implement appropriate safeguards to ensure the *integrity*, *availability,* and *confidentiality* of *assets* accessed and/or maintained using cloud computing services. The specific *administrative* and *technical safeguards* adopted should be commensurate with the institution's *risk assessment*.

4. Requirement I4 – Review and Approval of Proposed Information Systems

All proposed *information systems* and/or proposed modifications to *information systems* that *use* LSU *assets*, whether such *information systems* are to be procured with LSU funds (including donations, grants etc.), obtained from freely available services or developed internally, shall be submitted by *asset owner* (See Section B) to the respective LSU institution’s department/unit responsible for *Information Security*. The department/unit responsible for *Information Security* shall carry out a *risk assessment* involving all aspects of the *information systems* and determine appropriate measures required to be in compliance with institution or *Enterprise* policies.

Asset owners or prospective *owners* must acknowledge the *risk assessment* findings and work to implement appropriate *controls* to mitigate the *risk*. Any acceptance of *risk* must be documented and retained. Exceptions must be submitted where necessary as outlined in Policy A.

5. Requirement I5 – Internal System Connections

Each LSU institution shall develop written policies and procedures to explicitly authorize external connections to internal resources, and document, for each connection:

- Security requirements
- The nature of the information communicated

6. Requirement I6 – Secure Development Policy

Each LSU institution shall develop a secure development *policy* to ensure that *information security* is integrated within the software development lifecycle of all

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* that may access, process, store, or communicate the LSU institution's information.

2. Requirement J2 – Monitoring and Review of Supplier Services

Each LSU institution shall *monitor* applicable *suppliers* to ensure service delivery meets the *requirements* in accordance with Requirement J1.

3. Requirement J3 – Managing Changes to Supplier Services

Each LSU institution shall review any changes to the provision of services by applicable *suppliers* to determine what impact, if any, there may be to the *requirements* in accordance with Requirement J1.

4. Requirement J4 – Institution's Security Changes Impacting Supplier Services

Any changes to the LSU institution's *information security policy*, procedures, and *controls*, with the potential to impact applicable *suppliers* shall be communicated to ensure minimal disruption of services.

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 analysis, at each institution will be presented to the *Executive Management* for approval.

2. Requirement L2 – Testing the Disaster Recovery and Business Continuity Plan

Each LSU institution shall develop written procedures to test and revise the Disaster Recovery and Business Continuity Plan periodically to ensure the plan will be effective in the event of a *disaster*. Disaster Recovery and Business Continuity Plan testing shall occur no less frequently than every two years.

Documentation of Disaster Recovery and Business Continuity Plan tests shall be maintained in accordance with applicable laws and regulations.

3. Requirement L3 – Post Disaster Analysis

Each time the Disaster Recovery and/or Business Continuity Plan is activated in response to a *disaster* and the recovery is complete, the affected LSU institution shall conduct a post *disaster* analysis.

Each LSU institution shall maintain documentation of each post *disaster* analysis in accordance with applicable laws and regulations.

4. Requirement L4 – Processes and Procedures

Each LSU institution shall implement written *processes* and procedures to ensure that the *integrity*, *availability*, and *confidentiality* of critical *information system processes* including but not limited to protected and *restricted data* is maintained before, during, and after a *disaster*.

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
- Possess a level of awareness on information security relevant to their roles and responsibilities
- Receive updates on information security on an evolving and ongoing basis as events warrant. Updates may occur in any form or media that is appropriate

4. Requirement M4 – Institution's Compliance with Security Policies and Standards

Each LSU institution shall regularly *review* the compliance of information processing and procedures within their area of responsibility with regards to *PM-36* and any *subsidiary policies*, standards, and any other security *requirements*. If any non-compliance is found because of the *review*, the institution shall:

- Identify the causes of the non-compliance
- Evaluate the need for actions to achieve compliance
- Implement appropriate corrective action(s)
- Review the corrective action(s) taken to verify its effectiveness and identify any deficiencies or weaknesses.

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 requirement* was designed to defend against.

Each institution shall address any additional *risks* imposed by not adhering to the original *PM-36 requirement*.

2. Requirement N2 – Documentation of Compensating Controls

Each LSU institution shall thoroughly document each instance of compensating controls in use to ensure that the compensating control is achieving acceptable results in relation to the control specified in *PM-36* and in alignment with the institution's *risk management* program.