PERMANENT MEMORANDUM 50:
REVIEW AND APPROVAL FOR
ACQUISITION OF SOFTWARE AND SERVICES

POLICY DIGEST
Monitoring Unit: Office of Information Technology Services
Initially Issued: June 30, 2021

I. PURPOSE

Information Technology (IT) is vital to the effective operation of the University in fulfilling its mission. The University recognizes the volatility and interconnectedness of the IT environment requiring due diligence in acquisitions of software and services, including Internet of Things (IoT) solutions, to reduce the threat of security risks and data breaches, adhere to regulatory requirements, determine compatibility with IT infrastructure, and manage IT assets to promote effective use of IT investments. This policy identifies the expectations for each LSU institution to promulgate policies and procedures for the review and approval of software and services prior to acquisition.

II. DEFINITIONS

For purposes of this policy, and subsequent related institutional policies, the following definitions apply:

Accessible - refers to a site, facility, work environment, service, or program that is easy to approach, enter, operate, participate in, and/or use safely and with dignity by a person with a disability

Americans with Disabilities Act (ADA) - ADA is a Federal civil rights law that prohibits discrimination against people with disabilities in everyday activities. The Department of Justice (DOJ) published the Americans with Disabilities Act (ADA) Standards for Accessible Design in September 2010. These standards state that all electronic and information technology must be accessible to people with disabilities.

Acquisition – All forms of acquiring software or services, including but not limited to purchases, leases, subscriptions, gifts, grants, donations, open source, freeware and other no cost options.

Enterprise Information Technology (IT) - refers to IT solutions, resources, and data that are shared by more than one LSU institution. Enterprise IT includes collaborative efforts amongst the technology staff, services, and support associated with Enterprise software systems and services used to store and manage data and processes,

regardless of whether hosted on-campus, in the cloud, or through shared services. This is accomplished through realized economies of scale, formally designed, tested, implemented and supported solutions, that run mission-critical software.

Family Educational Rights and Privacy Act (FERPA) – FERPA is a Federal law that protects the privacy of student education records.

Health Insurance Portability and Accountability Act (HIPAA) – HIPAA is a Federal law that protects the privacy and security of certain health information.

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.

Internet of Things (IoT) - The Internet of Things refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

LSU Executive Information Technology Governance Council (EITGC) – The LSU EITGC provides strategic oversight to ensure IT strategies and resources are in alignment with stated goals. The EITGC is responsible for the development and maintenance of appropriate University-wide IT policies and plans as well as compliance in these matters by each LSU Institution.

LSU Institutions – All entities of the Board of Supervisors of the Louisiana State University and Agricultural and Mechanical College (LSU) as defined by the Bylaws.

Payment Card Industry (PCI) - The PCI Security Standards have been mandated by major credit card providers and is intended to protect cardholder data. For purposes of this policy, PCI compliance applies to any shopping cart and/or payment processing software that is installed on an institutionally owned computer, including customized, pre-installed, and "off-the-shelf" software and wireless devices. The following link provides a complete list of PCI approved Payment Application vendors: https://www.pcisecuritystandards.org/.

Protected Data - includes, but is not limited to, the following:

- Personally identifiable information (PII): includes but is not limited to Social Security Numbers, credit card numbers, bank and credit union account numbers, health insurance plan identification numbers, driver’s license numbers, dates of birth, and other similar information associated with an individual student or employee that, if misused, might enable assumption of that individual's identity

("identity theft") to compromise that person's personal or financial security.

- Protected health information (PHI): includes health information that is associated with at least one of eighteen identifiers that make the information “individually identifiable.” The eighteen identifiers specified by HIPAA include name, address, SSN, date of birth, date of health care, and other elements. Health information about groups of people (population data, mean and median data, aggregate data, etc.) that cannot be related to individuals is not PHI.

- Student educational record information: includes records that are based on student status and maintained by the institution or a party acting for the institution. Access to student records is governed by the Family Educational Rights and Privacy Act (FERPA).

- PCI data is defined by the Payment Card Industry Security Council as a Credit Card number (primary account number) and one or more of the following: Cardholder Name, Service Code, and Expiration Date.

- Gramm-Leach-Bliley Act (GLB Act or GLBA): requires that financial institutions act to ensure the confidentiality and security of customers’ “nonpublic personal information,” or NPI. Nonpublic personal information includes Social Security numbers, credit and income histories, credit and bank card account numbers, phone numbers, addresses, names, and any other personal customer information received by a financial institution that is not public.

- Protected Research Data: includes but is not limited, data gathered, generated, obtained, utilized, processed, and/or stored for the purposes of academic research or used for administrative purposes, which includes stipulations from the data owner or through contractual agreements. Examples of such data include, but is not limited to, Human subjects research data that identifies individuals, data classified as confidential by the researcher, contracting agency, or sponsor, data provided by an external party (public or private) with contractual stipulations.

Software – Data or instructions organized in the form of operating systems, utilities, programs, and applications that enable computers and related devices to operate.

Software and Services – Software and services is broadly defined to include software, Software as a Service (SaaS), subscriptions, software licenses, Internet of Things (IoT) solutions, and cloud-based services or any service and functionality delivered across the Internet with underlying hardware, software, and/or infrastructure supported by an external service provider.

University - The term University refers to the collection of campuses, academic programs, facilities, and other assets governed by the Board of Supervisors of the Louisiana State University and Agricultural & Mechanical College (LSU) as defined by

the Bylaws.

III. GENERAL POLICY

A. Scope

This policy applies to the review and approval of software and services (1) at all levels of application, including Enterprise, institution, unit, or individual and (2) across all types of acquisitions.

All Enterprise software and services acquisitions must be vetted through the LSU IT governance structure with final confirmation coming from the EITGC. Each LSU institution must implement related institutional policies and procedures with regard to software and services acquisitions by the institution, unit, or individual:

- Protect the organization from security risks and vulnerabilities;
- Ensure compliance with regulations, laws, and policies;
- Promote cost-savings; and
- Adhere to industry best practices.

B. Executive Information Technology Governance Council (EITGC)

At a minimum, the LSU EITGC establishes related policies and procedures, as applicable, to ensure all Enterprise software and services acquisitions are vetted in a manner that manages and balances the demand for Enterprise IT needs across the University while adhering to the required reviews for accessibility, information security, protected data, PCI, licensing agreements, and others, as appropriate. If software and services acquired initially by a single LSU institution are expanded to Enterprise, reviews shall be conducted in conjunction with the LSU EITGC to reaffirm compliance across all areas of review prior to expansion.

C. Institutional Policy

At a minimum, each LSU institution must establish a policy for reviewing software and services requests prior to acquisition, including the following requirements:

1. Define the scope, related definitions, and criteria for compliance with this policy in alignment with the institutional mission. Criteria may include, but is not limited to: level of risk, data classifications, intended use, audience, and/or other considerations, as appropriate.

2. Designate responsibility to conduct each type of institutional review prior to approval of software and services acquisitions. The following types of review are required by all LSU institutions:
    - **Accessibility:** Compliance for accessibility and usability standards (e.g., ADA).
    - **Information Security:** Compliance for security, privacy, and risk standards.
    - **Protected Data:** Assessment of potential for data breaches and to obtain data steward approval
    - **Payment Card Industry (PCI)**: Compliance for any software or service that collects payments (e.g., credit card use)

- **Licensing Agreements:** Review agreement language to ensure meets institutional standards.

Each LSU institution should conduct other types of reviews, as applicable, including but not limited to:

- **Compatibility:** Assessment of compatibility with IT infrastructure, including integrations with Institution-wide applications.
- **Duplication:** Consideration of existing software or services to meet requestor's needs, making efficient and effective use of technology investments

D. Oversight

The LSU EITGC provides oversight to ensure each LSU institution promulgates appropriate institutional policies and related procedures in adherence to this policy.

At a minimum, the Chief Information Officer, or similar role, at each LSU Institution shall be responsible for overall institutional compliance with this policy. However, additional areas of oversight may be appropriate, as determined by the institution.

E. Policy Enforcement

Failure to comply with this policy may subject the violator to loss of privileges and/or disciplinary action.

IV. PROCEDURES

Each LSU institution must develop and implement related policies and procedures in compliance with this policy.

Wherein opportunities may exist to utilize Enterprise applications to facilitate and streamline these procedures, institutions shall work collaboratively to ensure appropriate fit to meet each institution's needs.

V. SOURCES

PM 36