POLICY STATEMENT 286
REVIEW AND APPROVAL FOR
ACQUISITION OF SOFTWARE AND SERVICES

Revision: 2
Last Reviewed: May 24, 2023
Effective: May 24, 2023

PURPOSE:

The purpose of this policy is to provide guidelines for:

A. Complying with Louisiana State University (LSU) Permanent Memorandum 50 (PM-50), Review and Approval for Acquisition of Software and Services.

B. Establishing the guidelines for the review and approval for acquisition 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.

DEFINITIONS:

For purposes of this policy, 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.

LSUA Information Technology (IT) Governance – The LSUA IT Governance committee provides strategic oversight to ensure IT strategies and resources are in alignment with stated goals.

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.

STATEMENT OF POLICY:

As per the directives within Permanent Memorandum 50 (PM-50), all software and online/cloud-based service acquisitions must go through a formal review process. These requirements apply to both free and paid for software and services, as well as at all levels of use, including Enterprise-wide, institutional, unit, and individual. These acquisitions must be vetted and approved by a designated review team within each corresponding institution's IT unit to ensure that they do not violate data governance policies put forth by the State of Louisiana, LSU System/Enterprise, LSUA and cooperating 3rd party entities.

LSUA IET Services shall review the procurement of software and services (1) at all levels of application, including enterprise, institution, unit, or individual and (2) across all types of acquisitions, for the purposes of:

- Protecting the organization from security risks and vulnerabilities.
- Ensuring compliance with regulations, laws, and policies.
- Promoting cost-savings.
- Adhering to industry best practices.

GENERAL POLICY:

Users requesting software or cloud-based services will need to submit a request using IET's Software Request Form. Each submission will trigger an automated email to the requestor from our help desk acknowledging the receipt of the submission. Requestors should submit any follow-up inquiries regarding the status of an existing request in the form of a reply to the original automated email. All communications will be logged as part of the case record for each corresponding request in order to fully document the request and review process from beginning to end.

A. LSUA IET Services shall conduct a review, documenting the following detail:
    a. Intended use: How will the software or services be used by the end users.
    b. Intended audience: Who will use the software or services.
    c. Type of data: What type of data will be maintained, transmitted, or stored by the software or service.
    d. Compatibility: Assessment of compatibility with IT infrastructure, including integrations with other applications.
    e. Duplication: Consideration of existing software or services to meet requestor's needs, making efficient and effective use of technology investments.
    f. Accessibility: Compliance for accessibility and usability standards (e.g., ADA).
    g. Information Security: Compliance for security, privacy, and risk standards.
    h. Protected Data: Assessment of potential for data breaches.
    i. Payment Card Industry (PCI): Compliance for any software or service that

collects payments (e.g., credit card use).

j. Licensing Agreements: At the appropriate step in the review process, which may not be until after the software or services are approved for acquisition, review agreement language to ensure meets institutional standards.

B. LSUA IET Services shall submit the request for acquisition of software or services to the LSUA IT Governance Committee for review.

C. The LSUA IT Governance Committee will determine the level of approval needed for the software or services being acquired.

D. If the LSUA IT Governance determines the software/service should be an enterprise level acquisition, the LSUA Chief Information Officer (CIO) shall submit the software or services acquisition request to the appropriate level of LSU IT governance for approval.

POLICY ENFORCEMENT:

If a non-approved software purchase is made, the purchase plus the associated sales tax may be payroll deducted. Failure to comply with this policy may result in disciplinary action up to and including termination.

REFERENCES:

Permanent Memorandum - 50 (LSU)

APPROVED: _____
Paul Coreil, Ph.D., Chancellor

5/24/22
Date