Standard for Acquisition and Assessment of Technology Systems

November 2021

Purpose:

This standard outlines the process for requesting new systems and uses of technology at JMU regardless of their cost. The process will be used to evaluate new systems as well as current systems that are being expanded or renewed.

Definitions:

Higher Education Community Assessment Tool (HECVAT): The HECVAT is a questionnaire framework specifically designed for higher education to measure vendor risk. Prior to the purchase of a third-party solution, the vendor completes a HECVAT to confirm information, data, and cybersecurity policies are in place to protect sensitive institutional and constituent data. JMU prefers the full (vs. lite) version of the HECVAT. For easy use, a copy is available here along with other HECVAT tools.

SOC 2: A Service Organization Control 2 (SOC 2) is an auditing procedure conducted by an independent third-party auditor to ensure service providers securely protect the data and interests of the institution. A SOC 2 reports on various controls of the service organization related to security, availability, processing integrity, confidentiality, and privacy. JMU prefers the SOC 2, Type 2 for its assessments; however, other types of SOC reports may be acceptable.

System Classification: A classification is assigned to a system for risk management and security purposes based on the sensitivity level of the data as well as the impact to the university should the data be improperly disclosed, altered, or destroyed without authorization. System classifications are assigned by Information Technology with input from the data manager(s). A system may receive a classification of 1 – 4 with class 1 being assigned to systems containing highly confidential data, classes 2 and 3 for protected data, and class 4 for public data.

Standard:

1. Pre-Planning:

Those planning for new technology systems must begin early and give up-front consideration to the following items:

- **Existing solutions:** Determine if there is something already on campus that meets the need. If so, consider using it or be prepared to justify the need for a new product.
- **Funding:** Validate that a source of funding is available. Be sure to consider initial purchase costs as well as on-going/cost to continue requirements.
- **Approval:** Department head approval is required when a Technology Solution Request (TSR) is submitted.

2. Technology Solution Request:

University departments must submit a Technology Solution Request (TSR) prior to evaluating, procuring, or renewing any software. Additionally, a TSR must be submitted for the development or implementation of any new technology. There are two options available when submitting a TSR in the IT Service Portal:

- General Technology Solution Request: Used to request services of IT that are not related to procurement. Examples include implementing new services that require IT support, requesting review of services, or processes requiring IT support.

- Technology Procurement Request: Allows the requestor to provide the necessary information needed to perform the appropriate security review of the application or service being considered for purchase. This type of TSR should also be submitted to add new functionality to a system that has already been procured. It is not required for a software renewal unless IT was not involved in the original purchase.

For the purpose of this Standard, a Technology Procurement Request must be submitted containing detailed information such as:

- System Name, Type, and Description
- Estimated Cost
- Procurement Contact Name
- Vendor Name and Contact Information
- Data Elements Stored or Processed in the System
- System Interfaces
- Users of the System and Plan for Accessing the System
- Process for Creating and Managing User Accounts
- Names of Department Head (System Owner) and System Administrator

3. System Classification:

Once the TSR is received, an IT Sponsor will be assigned to work with Procurement and help facilitate the risk assessment process within IT. The IT Sponsor will also work with the appropriate data manager(s) to evaluate the data management and other compliance requirements that may be associated with the system and apply a system classification (1-4).

4. Acquisition:

Regardless of cost and whether the system will be acquired through small purchase, existing contract, or competitive procurement, the requestor should consult with JMU Procurement Services for advice on purchase and licensing options.

In no case shall individuals sign or otherwise agree to licensing terms or contract documents on behalf of the university.

5. Risk Assessment:

As the acquisition process begins, IT is required to complete and document an Information Security Risk Assessment. The level of assessment necessary is based on the system classification. Depending on the classification, the requestor will work with the vendor to collect and share with IT the necessary risk assessment documentation as follows:

Class 1 Systems	Class 2 Systems	Class 3 and 4 Systems
License Agreement	License Agreement	License Agreement
Privacy Policy and Terms of Use	Privacy Policy and Terms of Use	Privacy Policy and Terms of Use
JMU IT Services Addendum or equivalent terms and conditions deemed acceptable by IT and Legal Services	JMU IT Services Addendum or equivalent terms and conditions deemed acceptable by IT and Legal Services	JMU IT Services Addendum or equivalent terms and conditions deemed acceptable by IT and Legal Services
Completed Full HECVAT or equivalent questionnaire deemed acceptable by IT	Completed Full HECVAT or equivalent questionnaire deemed acceptable by IT	
SOC 2 report or other independent security audit deemed acceptable by IT	Optional: SOC 2 report or other independent security audit deemed acceptable by IT	
Data Control Procedures: Since Class 1 Systems contain highly confidential data that needs special treatment, the department must work in conjunction with IT and the appropriate data manager(s) to develop special handling procedures describing how the department will meet necessary compliance requirements. Primary examples include those involving: • Protected Health Information (PHI) covered by HIPAA • SSN and other highly confidential data To better understand these requirements, the department should email iso@jmu.edu for assistance.		

As IT completes the risk assessment process and necessary mitigations are identified, they will be shared with the system owner for acceptance and implementation. If at any point during implementation, it becomes apparent that the mitigations cannot be realized, the system owner must consult IT for assistance.

Depending on the scope and complexity of the system, potential risks surrounding it, and to preserve continuity of operations, IT reserves the right to set additional requirements or take on central management of any university system.

Provided the necessary information is made available, IT will process Class 3 and 4 systems as soon as practical using an abbreviated Operations Review assessment process. This generally occurs within a minimum of 2 weeks after TSR receipt.

For Class 1 and 2 systems, IT will not schedule the risk assessment until the necessary documentation is available and the system classification is confirmed (and in the case of a competitive procurement (RFP), until the preferred offeror(s) is identified). Requestors should allow at least 4 weeks after IT has received the necessary documentation for the risk assessment process to be completed.

6. Risk Acceptance:

Vendors unable to provide the required documentation listed in Section 5 will be considered high risk. Purchases from high risk vendors will require an additional approval/risk acceptance process. This process is as follows:

- Requestor must provide a written business justification to IT for the procurement or continued use of the system or service. Justification must also include approval from the requestor's Department Head (System Owner).
- The business justification and feedback/recommendation from IT's Technology Review Board is provided to the following individuals for their review and acceptance of the identified risk. Risk acceptance will be requested in the order listed below and is required from all individuals. If the required risk acceptance is not received, the TSR will be denied.
    - Data Manager(s)
    - Information Security Officer (ISO)
    - AVP for IT/CIO
    - Requestor's Vice President
    - Senior Vice President for Administration and Finance

New purchases of Class 1 systems from high risk vendors is not allowed.

Existing Class 1 systems provided by vendors deemed high risk may be allowed with the understanding that the system owner is required to work with IT and Procurement Services to encourage the vendor to complete and provide the necessary documentation to become compliant. This allowance may be provided for the duration of the contract. Upon contract expiration, system owners may be required to find an alternative solution should the vendor still be non-compliant.

7. On-going Risk Management:

To help ensure appropriate risk management continues over time, system owners are required to contact IT prior to any additions or changes to systems after they are acquired and to fully participate in collecting information as necessary to support annual system reviews performed by IT.