Standard for Acquisition and Assessment of Technology

November 2023

Purpose:

This standard outlines the process for requesting new systems and uses of technology at James Madison University (JMU) regardless of their cost, including technology made available to the University at no cost. The process is used to evaluate new technology as well as existing technology that is being expanded.

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 Information Technology (IT) prefers the full (vs. lite) version of the HECVAT.

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 IT prefers the SOC 2, Type 2 for its assessments; however, other types of independent security audits may be acceptable.

System Classification: A classification is assigned to a technology/system for risk management and security purposes based on the sensitivity level of the data as well as the impact to the University if the system were to become unavailable or if the system data would be improperly disclosed, altered, or destroyed without authorization. System Classifications are assigned by Information Technology (with input from the Data Manager(s) as needed). A system may receive a classification of 0 – 4 with class 1 being assigned to systems containing highly confidential data, classes 2 and 3 for protected data, class 4 for public data, and class 0 being assigned for desktop software or database subscriptions that process or store non-confidential data.

Standard:

1. Pre-Planning:

Those planning for a new technology solution/system must begin early and consider the following items:

- **Existing solutions:** Determine if an existing campus technology can meet the requestor's need and if so, the existing campus technology should be used, or the requestor should be prepared to justify the need for a new solution.
- **Funding:** Validate that a source of funding is available. Be sure to consider initial purchase costs as well as the ongoing cost of the technology.
- **Approval:** Director/Academic Unit Head (AUH) approval is required prior to a Technology Solution Request (TSR) being submitted.

2. Technology Solution Request:

University departments must submit a Technology Solution Request (TSR) prior to evaluating, or procuring a technology. Additionally, a TSR must be submitted prior to the development or implementation of any new technology. The TSR allows the requestor to provide the necessary information needed for IT to perform the appropriate security and business impact review of the technology being considered for use. The TSR should also be submitted to add new functionality to an existing technology . It is not required for the renewal of a technology contract unless IT did not perform a security review prior to the initial purchase and/or use.

For the purpose of this Standard, a TSR must be submitted by the requestor that includes detailed information such as:

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

3. System Classification:

Once the TSR is received, IT Policy and Compliance will work to facilitate the risk assessment process within IT. IT Policy and Compliance will work with the appropriate data manager(s), as needed, to evaluate the data management and other compliance requirements that may be associated with the system and apply a System Classification (0-4).

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 Procurement Services for guidance on purchase and licensing options. This includes agreements/licensing for technology that are at no cost to the University.

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 will complete and document an Information Security Risk Assessment. The level of IT assessment required is based on the System Classification. Depending on the classification, the requestor will work with the vendor and Procurement Services 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	JMU IT Services Addendum or equivalent terms and conditions deemed acceptable by IT	JMU IT Services Addendum or equivalent terms and conditions deemed acceptable by IT
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	
Completed System Management Plan that describes the regular activities, roles, and responsibilities essential to the support and maintenance of the system. The System Owner and System Administrator 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 and document these in the System Management Plan. Primary examples include those involving: • Protected Health Information (PHI) covered by HIPAA • Financial Data covered by the Gramm-Leach-Bliley Act (GLBA) • SSN and other highly confidential data	Completed System Management Plan that describes the regular activities, roles, and responsibilities essential to the support and maintenance of the system.	

As IT completes the risk assessment process and necessary mitigations are identified, they will be shared with the system owner for acceptance and implementation. The system owner must accept all identified mitigations before the TSR will be approved by IT. 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 (e.g. 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 continued use of the system or service. Justification must also include approval from the requestor's Department Head.
- 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
    - Vice President for Administration and Finance

New purchases of Class 1 systems from high-risk vendors are strictly prohibited.

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 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, which includes providing a completed System Management Plan.