University of Wisconsin Superior	Information Technology System and Services Acquisition Policy and Procedures	
Department Name Technology Services	Policy # IT-SA1	**Issue Date:** March 8, 2016
Approved by:		

1. Purpose

The University of Wisconsin Superior fosters intellectual growth and career preparation within a liberal arts tradition that emphasizes individual attention, embodies respect for diverse cultures and multiple voices, and engages the community and region. This policy establishes the Information Technology System and Services Acquisition Policy and Procedures. This policy addresses the establishment of procedures for the effective implementation of selected security controls and control enhancements in the System and Services Policy and Procedures family.

2. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by the University of Wisconsin Superior. Any information, not specifically identified as the property of other parties, that is transmitted or stored on University of Wisconsin Superior IT resources (including e-mail, messages and files) is the property of the University of Wisconsin Superior. All users (University of Wisconsin Superior employees, Students, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Data Classification

Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). Access Controls will vary depending upon the following classifications:

Level I: Low Sensitivity/Public Data:
Access to Level I institutional data is targeted for general public use and may be granted to any requester or may be published with no restrictions. Level I data is specifically defined as public in local, state, or federal law, or data whose original purpose was for public disclosure.

Examples of Level I (low sensitivity) institutional data:

- published "white pages" directory information
- maps
- university websites intended for public use
- course catalogs and schedules of classes (timetables)
- campus newspapers, magazines, or newsletters
- press releases
- campus brochures

Level III: Moderate Sensitivity/Internal Data:
Access to Level III institutional data is authorized for all employees for business purposes unless restricted by a data steward. Access to data of this level is generally not available to parties outside the university community and must be requested from, and authorized by, the data steward who is responsible for the data.

Examples of Level III (moderate sensitivity) institutional data:

- project information
- official university records such as final grades, financial aid awards, financial reports, etc.
- human resources information
- some research data
- unofficial student records
- budget information

Level V: High Sensitivity/Restricted Data:

Access to Level V institutional data must be controlled from creation to destruction, and will be granted only to those authorized persons who require such access in order to perform their job, or to those individuals permitted by law. Access to Level V data must be individually requested and then authorized by the data steward who is responsible for the data. Level V data is highly sensitive and access to this data is restricted by laws such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights & Privacy Act (FERPA), Code of Federal Regulations Title 45, the Wisconsin Notification Act 138, and any other applicable federal or state laws. In law, Level V data elements are usually restricted due to a direct relationship to an individual's identity (such as name); however this policy requires restriction of the data elements themselves regardless of any link to an individual's identity.

Examples of Level V (high sensitivity) institutional data:

- social security numbers
- credit card numbers
- passwords
- individual health information or financial account information
- driver's license numbers or state identification numbers
- survey or research data covered by the Institutional Research Board (IRB) as defined by the appropriate data steward
- research and/or classes that deal with "personally identifiable information" as defined by the appropriate data steward
- any information containing biometric data that can identify an individual, such as DNA profile, fingerprint, voice print, retina or iris image, or unique physical characteristic

Level VI (Level III or Level V Authentication Data):

Authentication data used to access systems using Level III or Level V information must be controlled from creation to destruction, and will be granted only to those authorized persons who require such access in order to perform their job, or to those individuals permitted by law. Authentication data is assigned to individuals as codes or passwords or derived from their physical identity. Authentication data authorizes particular individual's access to selected

institutional systems and data. Authentication data must be stored as a one-way, salted hash with no record of the original document except in the case of a secure password management system. Authentication data is administrative in nature and must be stored and handled separately from other forms of institutional data.

Examples of authentication data include but not limited to:

- passwords
- biometric data including finger print, retina, voice, face, or some other scan of a physical characteristic
- access codes
- authentication tokens

4. Intent

The University of Wisconsin Superior Information Technology System and Services Acquisition Policy and Procedures serves to be consistent with best practices associated with organizational information security management. It is the intention of this policy to establish Information Technology System and Services Acquisition Policy and Procedures throughout the University of Wisconsin Superior to help the organization implement security best practices with regard to Level III, Level V or Level VI data.

5. Policy

The University of Wisconsin Superior has chosen to adopt the Information Technology System and Services Acquisition Policy and Procedures established in the National Institute for Standards and Technology (NIST) SP 800-53 "System and Services Acquisition Policy and Procedures," Family guidelines, as the official policy for this domain. The following subsections outline standards that constitute the University of Wisconsin Superior Services Acquisition Policy and Procedures.

- SA-3 System Development Life Cycle: All University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must be managed according to the systems development life cycle incorporating security considerations, roles, responsibilities and risk management throughout the life cycle.

- SA-4 Acquisition Process: Acquisition contracts used to procure University of Wisconsin Superior Information Systems that will use Level III, Level V or Level VI data must include the following requirements, descriptions, and criteria explicitly or by reference:
    - Security functional requirements
    - Security strength requirements

- Security assurance requirements
- Security-related documentation requirements
- Requirements for protecting security-related documentation
- Descriptions of the information system development environment and environment in which the system is intended to operate
- Acceptance requirements

- SA-5 Information System Documentation: All University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must have documentation that describes the following:

  - Secure configuration, installation, and operation of the system, component, or service.
  - Effective use and maintenance of security functions/mechanisms.
  - Known vulnerabilities regarding configuration and the use of privileged accounts.
  - User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
  - Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and user responsibilities for maintaining that security.
  - Methods used to obtain the documentation in the event that the documentation is unavailable or nonexistent.

  Documents must be protected and distributed to the appropriate Technology Services Personnel

- SA-8 Security Engineering Principles: All University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must have security engineering principles applied to their specification, design, development, implementation, and modification.

- SA-9 External Information System Services: When utilizing externally provided Information Systems or services that use Level III, Level V or Level VI data, the University of Wisconsin Superior must require the provider to comply with campus information security requirements and clearly define and document the roles and

responsibilities with regard to the external information system or service. In addition, the campus must monitor security control compliance by external service providers on an ongoing basis.

- SA-10 Developer Configuration Management: All developers working on University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must:
    - Document, manage, and control the integrity of changes to the system, component or service.
    - Implement only organization-approved changes to the system, component, or service.
    - Document approved changes to the system, component, or service and the potential security impacts of such changes.
    - Track security flaws and flaw resolution within the system, component, or service and report finding to Information Technology Management.

- SA-11 Developer Security Testing and Evaluation: All developers working on University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must:

    - Create and implement a security assessment plan that includes security testing/evaluation.

    - Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.

    - Implement a verifiable flaw remediation process that corrects flaws identified during security testing/evaluation.

- SA-12 Supply Chain Protection: All University of Wisconsin Superior Information Systems using Level III, Level V or Level VI must have reasonable protection against supply chain threats.

- SA-14 Criticality Analysis : All University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must be analyzed in order to identify critical information system components and functions

- SA-15 Development Process, Standards, and Tools: All developers working on University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must follow a documented development process that:

- Explicitly addresses security requirements.
- Identifies the standards and tools used in the development process.
- Documents the specific tool options and tool configurations used in the development process.
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

Information Technology Management will review the development process, standards, tools and tool options/configurations to determine if they satisfy the campus security requirements.

- SA-17 Developer Security Architecture and Design: All developers working on University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must produce a design specification and security architecture that:
  - Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture
  - Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components
  - Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.