University of Wisconsin Superior	Information Technology Personnel Security Policy and Procedures	
Department Name Technology Services	Policy # IT-PS1	**Issue Date:** March 16, 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 Personnel Security Policy and Procedures. This policy addresses the establishment of procedures for the effective implementation of selected security controls and control enhancements in the Personnel Security 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 Personnel Security 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 System and Communication access control capabilities 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 Personnel Security Policy and Procedures established in the National Institute for Standards and Technology (NIST) SP 800-53 "Personnel Security," Family guidelines, as the official policy for this domain. The following subsections outline the Access Control standards that constitute the University of Wisconsin Superior Information Technology Personnel Security Policy and Procedures.

- PS-4 Personnel Termination: All personnel who are no longer employed by the University of Wisconsin Superior and who have elevated privileges to Information Systems using Level III, Level V or Level VI data must:
    - Have their access to the information system disabled immediately upon termination.
    - Have any authenticators/credentials revoked.
    - Turn in all security-related organizational information system property to the Technology Services Department.
- PS-5 Personnel Transfer: All personnel who are transferred or reassigned to other positions within the organization and who had access to Information Systems using Level III, Level V or Level VI data must have:

  - Their operation need for ongoing logical and physical access reviewed by their previous supervisor, new supervisor and convey any changes to Technology Services and/or Facilities Management.
  - Their access modified as needed to correspond with any changes in operational need due to reassignment or transfer.

- PS-7 Third-Party Personnel Security: All Third-Party organizations with personnel that have elevated privileges to University of Wisconsin Superior Information Systems using Level III, Level V or Level VI data must comply with university security policies and procedures and notify the campus when aforementioned personnel have terminated employment or change roles with the organization.