University of Wisconsin Superior	Information Technology Physical and Environmental Access Control Policy	
Department Name Technology Services	Policy # IT-PE1	**Issue Date:** February 29, 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 Physical and Environmental Access Control Policy for the effective implementation of selected security controls and control enhancements for managing risks associated with the physical and environmental profile of campus information systems.

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 Physical and Environmental Access Control Policy serves to be consistent with best practices associated with organizational information security management. It is the intention of this policy to establish Physical and Environmental access control capabilities throughout the University of Wisconsin Superior to help the organization implement security best practices with regard to the Physical and Environmental Security of Level III, Level V or Level VI data.

5. Policy

The University of Wisconsin Superior has chosen to adopt the Physical and Environmental Access Control principles established in the National Institute for Standards and Technology (NIST) SP 800-53 "Physical and Environmental Protection," Family guidelines, as the official policy for this domain. The following subsections outline the Access Control standards that constitute the University of Wisconsin Superior Physical and Environmental Access Control Policy.

- PE-2 Physical Access Authorizations: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must:
    - Develop, approve, and maintain a list of individuals with authorized access to the facility where the information resides.
    - Issue authorization credentials for facility access.
    - Review the access list detailing authorized facility access by individuals every six months and remove individuals from the facility access list when access is no longer needed.
- PE-3 Physical Access Control: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must:
    - Enforce physical access authorizations at entry/exit points.

  - Maintain physical access audit logs and/or video surveillance footage at entry/exit points.
  - Escort visitors and monitor their activity.
  - Secure keys, combinations, and other physical devices.
  - Inventory access tokens every six months.
  - Change combinations, keys or tokens when they are lost, compromised, or individuals are transferred or terminated.
- PE-4 Access Control for Transmission Medium: All custodians of University of Wisconsin Superior transmission mediums transporting Level III, Level V or Level VI data must control physical access to the medium by:
  - Maintaining locked wiring closets.
  - Disconnecting unused spare data jacks.
  - Protecting distribution layer medium using conduit or cable trays.
  - Locating and removing network hubs.
  - Placing configurable network devices located in publically accessible areas inside of locked containers.
- PE-5 Access Control for Output Devices: All custodians of University of Wisconsin Superior output devices such as printers, facsimile machines, copiers, monitors, scanners and audio devices using Level III, Level V or Level VI data must control physical access to the devices and ensure that only authorized individuals receive output from the devices.
- PE-6 Monitoring Physical Access: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must:
  - Monitor physical access to the facility where the information system resides to detect and respond to physical incidents.
  - Review physical access logs and report events of interest to campus safety officers.
- PE-9 Power Equipment and Cabling: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must protect the power equipment and cabling from damage and destruction.
- PE-10 Emergency Shutoff: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must:
  - Provide the capability of shutting off power to the information system or individual system components in emergency situations
  - Place emergency shutoff switches in a highly visible location with the appropriate signage.
  - Protect emergency shutoff capability from unauthorized access.

- PE-12 Emergency Lighting: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must employ and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
- PE-13 Fire Protection: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
- PE-14 Temperature and Humidity Controls: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must maintain and monitor temperature and humidity levels within the facility where the information system resides.
- PE-15 Water Damage Detection: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
- PE-16 Delivery and Removal: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must authorize, monitor, and control information systems entering and exiting the facility and maintain records of those items.
- PE-18 Location of System Components: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must position information system components within the facility to minimize potential damage from environmental hazards and to minimize the opportunity for unauthorized access.
- PE-19 Information Leakage: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must protect information systems from information leakage due to electromagnetic signal emanation.
- PE-20 Asset Monitoring and Tracking: All custodians of University of Wisconsin Superior Facilities containing systems using Level III, Level V or Level VI data must employ video surveillance to track and monitor the location and movement of information systems.