University of Wisconsin-Stevens Point
Information Technology

Institutional Data Access and Protection Policy

Policy No. 1
Date Drafted: 02/19/2008
Date Approved: 02/02/2009
Last Date Revised/: 04/26/2019

Status	**Responsible University Office**
☐**Draft**	Data Stewards
☐**Under Review**	
☑ **Approved**	**Responsible Coordinating Office**
☐ **Obsolete**	Information Technology

1. Policy Purpose

The purpose of this policy is to establish consistent requirements to protect data and govern data *access*. This policy establishes a standard definition of *sensitive data* and security precautions needed to protect that data. Other key elements of *data governance* including the roles and responsibilities of data stewardship and the process for obtaining and securing appropriate access are further defined in the Institutional Data Access and Protection Roles and Responsibilities Policy.

Institutional data is information that supports the mission and operation of the University of Wisconsin-Stevens Point. It is the responsibility of the University of Wisconsin-Stevens Point to implement policies and procedures to provide necessary access to institutional data while at the same time ensuring *confidentiality*, *integrity*, and accountability of the information. Institutional data is essential and its protection must be ensured to comply with legal, regulatory, and administrative requirements. This policy is a basis for complying with federal and state laws such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights & Privacy Act (FERPA), and Wisconsin Notification Act 138.

(**NOTE**: Phrases shown in *italics* at their first occurrence in this document are defined in the associated IT Common Definitions document)

2. Policy Scope

All data (electronic, paper, spoken, or otherwise) used to conduct university operations and meet its educational, business, and research goals are governed by this policy. This includes data gathered, given, received, or used by *employees*, students, and/or affiliates for purposes of administrative, instructional, or research use. Also included is all licensed, purchased, or leased data.

- Examples of data gathered, given, or received include but are not limited to: student data for instructional or administrative use, personnel and payroll data, financial and budget data, and data available from the university web sites, printed on paper copy or written.

- Examples of licensed purchased or leased data include but are not limited to: geographic data sets, postal mailing addresses, and survey results data.

3. Policy Statement

Chief data stewards are the senior administrative officers of the University of Wisconsin-Stevens Point and are responsible for overseeing all institutional data resources. Their designees, the data stewards, are accountable for managing institutional data access, assessing institutional risks and threats to the data for which they are responsible, and for classifying its relative sensitivity as Low Risk (low sensitivity), Moderate Risk (moderate sensitivity), or High Risk (high sensitivity). Unless otherwise classified, institutional data is Moderate Risk. University personnel may not copy, replicate, or otherwise propagate High Risk institutional data without prior approval of the appropriate data steward. Data stewards can request assistance from the *Information Security Office* in classifying their data and advice about available controls.

- Institutional data must be protected from unauthorized disclosure, modification, or destruction.
- Permission to access institutional data will be granted to all eligible university employees for legitimate university purposes. Legitimate university purposes and eligible employees will be determined by the data stewards based on appropriate university policy.
- Authorization for access to High Risk institutional data comes from the data steward and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other authority.
- Where access to institutional data has been authorized, use of such data shall be limited to the purpose for which access to the data was granted.
- University employees, students, and affiliates must report instances in which institutional data is at risk of unauthorized disclosure, modification, or destruction.
- All decisions regarding the collection and use of institutional data must be in compliance with the law and with university policies and procedures.
- Appropriate security practices, consistent with the data handling requirements in this policy, must be used to protect institutional data.
- Any individual granted access to institutional data is expected to observe ethical restrictions that apply to the information they access, and to abide by applicable laws and policies with respect to accessing, using, or disclosing information.
- University employees must read and acknowledge they have read the institution's confidentiality agreement educating them on sensitive data and their responsibilities regarding its protection.

3.1. Data Classification

Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). For each classification, several data handling requirements are defined to appropriately safeguard the information.

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

Examples of Low Risk (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

B. **Moderate Risk: Moderate Sensitivity:**

Access to Moderate Risk 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 Moderate Risk(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

C. **High Risk: High Sensitivity:**

Access to High Risk 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 High Risk data must be individually requested and then authorized by the data steward who is responsible for the data. High Risk 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, High Risk 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 High Risk (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

3.2. Data Handling

The following chart specifies security precautions needed to safeguard and protect institutional data for the three data classifications. The level of control in the following data handling areas depends on the classification of data.

Data Handling and Control Areas	Low Risk Low Sensitivity (Public Data)	Moderate Risk Moderate Sensitivity (Non-Public/Internal Data)	High Risk High Sensitivity (Confidential/Restricted Data)
Printed Reports	No controls	May be sent via campus mail; no labels required	Individually authorized, with a confidentiality agreement. Must be delivered via confidential courier; reports must be marked "confidential"
Electronic Access	No controls	Role-based authorization	Individually authorized, with a confidentiality agreement
Secondary Use	Authorization by data steward recommended	As authorized by data steward	Prohibited
Physical Data/Media Storage	No controls	Access is controlled	Access is controlled, monitored, and logged
External Data Sharing	No controls	As allowed by Wisconsin Open Records Law; FERPA restrictions	As allowed by Federal regulations; Wisconsin Open Records Law; FERPA restrictions; and *Business Associate Agreement* for Protected Health Information (PHI)
Electronic Communication / Transmission	No controls	*Encryption* recommended	Encryption required
Data Tracking	No controls	No controls	Social security numbers, credit cards, and PHI locations must be registered
Data Disposal	No controls	Recycle reports; wipe/erase media	Shred reports; *Department of Defense Level Wipe* or destruction of electronic media

Data Handling and Control Areas	Low Risk Low Sensitivity (Public Data)	Moderate Risk Moderate Sensitivity (Non-Public/Internal Data)	High Risk High Sensitivity (Confidential/Restricted Data)
Auditing	No controls	No controls	Audit logins and changes in access
Mobile Devices	No controls	Password protection recommended; locked when not in use recommended	Password protected; locked when not in use; encryption used for High Risk data
Personally Owned Devices	No controls	Password protection recommended; locked when not in use recommended; up-to-date virus protection and patches required	Prohibited

Printed Reports – A requirement for the heading on a printed report to contain a label indicating that the information is confidential, and/or a cover page indicating the information is confidential is affixed to reports.

Electronic Access – How authorizations to information in each classification are granted.

Secondary Use – Indicates whether an authorized user of the information may repurpose the information for another reason or for a new application.

Physical Data/Media Storage – The protections required for storage of physical media that contain the information. This includes, but is not limited to: workstations, servers, CD/DVD, tape, USB Flash drives, laptops, and PDAs.

External Data Sharing – Restrictions on appropriate sharing of the information outside of the University of Wisconsin-Stevens Point

Electronic Communication / Transmission – Requirements for the protection of data as transmitted over telecommunications networks.

Data Tracking – Requirements to centrally report the location (storage and use) of information with particular privacy considerations.

Data Disposal - Requirements for the proper destruction or erasure of information when decommissioned (transfer or surplus), as outlined in the Computer and Digital Storage Media Disposal Policy.

Auditing – Requirements for recording and preserving information accesses and/or changes, and who makes them. Audit records will be kept and reviews by appropriate staff.

Mobile Devices – Requirements for the protection of information stored locally on mobile devices. This includes, but is not limited to: laptops, tablet computers, PDAs, cell phones, and USB flash drives.

Personally Owned Devices – Requirements for the protection of information stored locally on devices owned by faculty or staff. This includes, but is not limited to: desktop computers, laptops, tablet computers, PDAs, cell phones, and USB flash drives.

4. Terms and Definitions

A common set of terms and definitions used in university-level IT policies are defined in the IT Common Definitions document.

5. Related Policies, Procedures, References, and Attachments

The collection of University of Wisconsin-Stevens Point IT policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Wisconsin-Stevens Point policy.

- IT policies and procedures are available at: http://www.uwsp.edu/it/about/policies/
- IT Procedure – Policy Development, Approval, and Implementation
- IT Reference – Common Definitions
- The Surplus Property Office – Surplus Property Disposal policy can be found at: http://www.uwsp.edu//Surplus/
- IT Policy –Institutional Data Access and Protection Roles and Responsibilities

Contact Information

For questions about this IT policy, contact the Information Security Office at Information.Security.Office@uwsp.edu or the Director of Information Technology/CIO.