University of Wisconsin-Stevens Point
Information Technology

Institutional Data Access and Protection Roles and Responsibilities Policy

Policy No. 2
Date Drafted: 02/19/2008
Date Approved: 02/02/2009
Last Date Revised: 07/27/2010

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

1. Policy Purpose
This document supports the Institutional Data Access and Protection Policy. The purpose of this policy is to define the roles and responsibilities of university employees who are responsible for data governance. This is the process by which the university manages the quality, consistency, usability, security, and availability of its data.

2. Policy Scope
The policies and procedures provided herein apply to all university employees including student employees. This policy governs the protection, privacy, security, and confidentiality of institutional data, especially highly sensitive data, and the responsibilities of institutional units and individuals for such data.

3. Policy Statement
Departments, units, or individuals that have stewardship responsibility for portions of internal and highly sensitive institutional data must establish internal controls to ensure that university policies are enforced. All data users, not just data stewards or administrators, are responsible for the protection, security, and privacy of the data they access, as prescribed in this policy.

Roles and Responsibilities:

Chief Data Stewards
Senior administrative officers are responsible for managing information resources while conducting university business. The provost and vice chancellor for academic affairs, vice chancellor for business affairs, and the vice chancellor for student affairs serve as the chief data stewards of institutional data. They delegate the policy-level responsibilities for data governance to the data stewards.

Chief data stewards are responsible to:

1. Establish policies and directions for the overall accessibility, security, and privacy of all institutional data, especially highly sensitive data within their respective areas of responsibility.
2. Identify and appoint data stewards for units within their areas of responsibility.

Data Stewards

Data stewards are individuals delegated responsibility by the chief data stewards to manage data used in their area (i.e., they are responsible for its accuracy, integrity, and implementation of policy and procedures for appropriate use and protection of the data). A list of data stewards and their data domains appear in appendix A.

Data stewards are responsible to:

1. determine security classification of all data managed in their areas as described in the Institutional Data Access and Protection Policy.
2. define access roles and assign access on a need to know basis.
3. grant access to data based on the Institutional Data Access Request Procedure.
4. annually review with appropriate data administrators the current set of highly sensitive data access authorizations and, as appropriate, update authority granted to each data user.
5. ensure that all department/unit personnel with access to information assets are trained in relevant security and confidentiality policies and procedures.
6. ensure compliance with institutional data security policies and procedures.

Data Administrators

Data administrators are individuals that have operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of institutional data. This includes the installation, maintenance, and operation of computer hardware, software, and database platforms. They work closely with the data stewards or their designees on implementation of institutional data policies, standards, and procedures.

Data administrators are responsible to:

1. define and implement processes for assigning and revoking data user access privileges and setting file protection parameters.
2. implement data protection and access controls conforming to the Institutional Data Access and Protection Policy.
3. define and implement procedures for backup and recovery of institutional data for which they are responsible.
4. ensure processes are in place for the detection of security violations.

Data Users

Data users are employees who have been granted permission to enter, modify, destroy, or access specific institutional data in the performance of their assigned duties is considered a data user. For the purposes of this policy, employees include permanent and limited term faculty, academic staff and classified staff, student employees, trainees, and volunteers.

Data users are responsible to:

1. refrain from asking for, collecting, or disseminating any High Risk data unless authorized or required by a data steward.
2. only use High Risk data for purposes for which they have been authorized.
3. seek access to High Risk data only according to the Institutional Data Access Request Procedure.
4. access only that data which they have a need to know to carry out job responsibilities.
5. alert data steward of any access privileges inappropriate to job duties.
6. treat any High Risk data securely by following the data handling practices defined in section 3.2 of the Institutional Data Access and Protection Policy.
7. never place High Risk data on personally-owned devices (cell phones, portable or desktop computers, etc.).
8. never place High Risk data on university-owned devices (cell phone, portable or desktop computers, etc.), unless authorized by a data steward.

Data users who are also employee supervisors are responsible for all of the above duties as well as making sure that those they supervise comply with the above responsibilities.

Information Technology Security Office
This office is responsible for ensuring and directing implementation of institutional data access and protection policies and procedures.

The information technology security officer is responsible to:

1. coordinate the development and maintenance of information security policies and standards.
2. investigate security incidents and coordinate their resolution.
3. implement an information security awareness program.
4. provide consulting services for information security throughout the University.
5. conduct assessments of compliance to institutional data access policies. Report violations to appropriate data steward and chief information officer (CIO).

4. Terms and Definitions

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

5. Related Policies, 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
- IT Policy - Institutional Data Access and Protection

- The Surplus Property Disposal Policy can be found at: http://www.uwsp.edu//Surplus/

Contact Information

For questions about this other information technology policies, contact the information security office at Information.Security.Office@uwsp.edu or the director of information technology/CIO.

University of Wisconsin-Stevens Point
Information Technology

Appendix A

CURRENT LIST OF PERSONS PERFORMING RELEVANT ROLES

MAJOR DATA DOMAINS	ROLE	PERSON	TITLE
STUDENT ACADEMIC RECORDS	Chief Data Steward	Bob Tomlinson	Vice Chancellor for Student Affairs
	Data Steward	Dan Kellogg	Registrar
STUDENT HEALTH RECORDS	Chief Data Steward	Bob Tomlinson	Vice Chancellor for Student Affairs
	Data Steward	Bill Hettler	Director, Health Services
ACADEMIC AFFAIRS PERSONNEL, BUDGET	Chief Data Steward	Mark Nook	Provost and Vice Chancellor for Academic Affairs
	Data Steward	Katie Jore	Associate Vice Chancellor for Personnel, Budget, Grants & Summer Session
EMPLOYEE AND PAYROLL INFORMATION	Chief Data Steward	Greg Diemer	Vice Chancellor for Business Affairs
	Data Steward	Robert Tabor	Director Personnel & Payroll Services
GENERAL FINANCIAL INFORMATION	Chief Data Steward	Greg Diemer	Vice Chancellor for Business Affairs
	Data Steward	Bo DeDeker	Controller
ACADEMIC/ INSTRUCTIONAL CONTENT	Chief Data Steward	Mark Nook	Provost and Vice Chancellor for Academic Affairs
	Data Steward	Katie Jore	Associate Vice Chancellor for Personnel, Budget, Grants & Summer Session
INFORMATION TECHNOLOGY	CIO	Dave Dumke	Director/CIO
	Information Security Officer	Peter Zuge	Security Officer

PLEASE NOTE: Educational records as defined by the federal Family Educational Rights and Privacy Act (FERPA) may include information from any of the major data domains listed above or additional data domains. It is the policy of the University that any education record be managed in accord with FERPA.