University of Wisconsin-Stevens Point
Information Technology

The following information is a portion of the document titled:
Institutional Data Access and Protection Policy

To view the document in its entirety, please click on the above link.

LEVEL III DATA

Level III: High Sensitivity:
Access to Level III 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 III data must be individually requested and then authorized by the data steward who is responsible for the data. Level III 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 III 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 III (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

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	Level 1 Low Sensitivity (Public Data)	Level II Moderate Sensitivity (Non-Public/Internal Data)	Level III 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
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 the Level III data
Personally Owned Devices	No controls	Password protection recommended; locked when not in use recommended; up-to-date virus protection and patches required	Prohibited