University of Wisconsin Stevens Point
Information Technology

Institutional Sensitive Data Storage Request

Procedure No 3

Date: Date Drafted: 02/27/2008
Date Approved: 05/14/2010
Last Date Revised: 05/08/2010

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

1. Procedure Purpose

This document is in direct support of the *Institutional Data Access & Protection Policy*. This document sets forth steps for requesting permission to store *Institutional Data*, and in particular to store High Risk *Sensitive Data* as defined in the Institutional Data Access and Protection Policy. This document shall be subject to periodic changes and updates, as necessary, independent of the policy document itself.

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

2. Procedure Scope

The procedure is intended to assist university employees with their responsibilities as described in the Institutional Data Access & Protection Policy. Permission to store institutional data is granted by Data Stewards who are required to develop and maintain clear and consistent procedures for use of the data, prevent unauthorized access, and protect High Risk sensitive data. Examples of these guidelines are found below as well as in the Employee Confidentiality Agreement.

3. Procedure

Data Stewards or designees grant permission to store sensitive data within their purview according to the following procedure. This ensures the Requestor is certified to view and retain sensitive data and has met appropriate pre-requisites, including training and acknowledgement of a Confidentiality Agreement.

3.1. Data User completes a Request for Storage of Sensitive Data form (see Appendix for sample form), and forwards it to their supervisor for approval and submission to the appropriate Data Steward.

3.2. Data Steward consults with the Information Security Office to assess the risk of exposure of the sensitive data and how it will be protected.

3.3. Data Steward reviews requests for required prerequisites, such as: i) *Data User* acknowledges having received the University's Data Access Policy; ii) Data User's

supervisor certifies that Data User needs to store Sensitive data based on job responsibilities, and verifies the accuracy of the information conveyed on the Request for Storage of Sensitive Data form.

3.4. If prerequisites have been met, the Data Steward determines if data sensitivity training is required, such as WISDM training, knowledge of Family Education Rights and Privacy Act (FERPA) and/or review of Gramm-Leach-Bliley Act (GLBA) Sensitive Data Access guidelines.

3.5. The Data Steward completes the form, instructs the Requestor how to protect the data, informs the Information Security Office and logs the request.

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 Office – Surplus Property Disposal Policy can be found at: http://www.uwsp.edu/Surplus/TermsAndPolicies.aspx#policies

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.

Appendix:

UNIVERSITY OF WISCONSIN-STEVENS POINT

REQUEST FOR STORAGE OF SENSITIVE DATA

EMPLOYEE / STUDENT NAME:	**DATE:**
EMPLOYEE / STUDENT ID:	**POSITION TITLE:**
DEPARTMENT:	**PHONE NUMBER:**

I request approval to store highly sensitive data. I acknowledge my responsibility to treat this data with the utmost care and meet all of the requirements specified in the Institutional Data Access and Protection Policy available at http://www.uwsp.edu/infosecurity/policies.

What type of sensitive data do you wish to store?
Check only one. Complete a separate form for each data type.

- ☐ Student SSN (send to Registrar)
- ☐ Employee SSN (send to Personnel Director)
- ☐ Credit Card Number (send to Controller)
- ☐ Financial account information (send to Controller)
- ☐ Health information (send to Health Services Director)
- ☐ Driver's License/ID (send to InfoSecurity Office)
- ☐ Passwords (send to InfoSecurity Office)

Describe why you wish to retain sensitive data (i.e. purpose):

Describe where this sensitive data will be located (i.e. laptop, network drive, desktop, file cabinet, etc.):

Describe the department or unit that this sensitive data originated from (if known). List any other departments or units with whom you are sharing this information.

Department Head Signature:
I certify that the requestor needs this access to do their job and the information on this request is accurate.

FOR DATA STEWARD USE ONLY	
☐ **APPROVED DATE:**	☐ **NOT APPROVED DATE:**
ACCESS GRANTED UNTIL:	**REASON FOR NON-APPROVAL:**
DATA STEWARD SIGNATURE:	