University of Wisconsin - Stevens Point
Information Technology

Sensitive Data Scan Procedure for Electronic Data

Procedure No. 5
Date Drafted: 12/04/2008
Date Approved: 06/18/2010
Last Date Revised: 06/18/2010

Status	**Responsible University Office**
☐ **Draft**	Information Security Office
☐ **Under Review**	
☒ **Approved**	**Responsible Coordinating Office**
☐ **Obsolete**	Information Security Office

1. Procedure Purpose
This procedure defines the process to identify *sensitive data* and the steps required to remove or protect sensitive data based on the Institutional Data Access & Protection Policy.

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

2. Procedure Scope
The scope includes identifying and remediating sensitive data on all employee workstations.

3. Procedure
The *Information Security Office* (ISO) provides access to data scan software, employee instructions and training material for running scans, reporting results and works with unit leaders to remediate results.

3.1. The ISO contacts each data steward to explain objectives and requirements for the removal or protection of sensitive electronic data including an explanation of each user's role and how the ISO will monitor the cleanup of workstations.

3.2. Deans and data stewards assign unit leaders for each area. They will explain the purpose of this effort, hand out this document as a brief introduction, and give them the authority and responsibility of removing sensitive data from area workstations.

3.3. The ISO meets with unit leaders to explain the overall sensitive data scanning process, the need for employees to scan their workstations, and the monitoring of results by the ISO. Unit leaders and the ISO will agree upon initial start dates and deadlines. The ISO will provide training materials.

3.4. ISO runs scan and sends scan results of the units to the unit leaders.

3.5. Unit leaders direct employees to review their workstation scan results and clean up data per training material.

3.6. If the employee determines they need to retain sensitive data on their workstation they fill out a Request for Access/Storage of Sensitive Data form and submit it to

their unit leader.

3.7. The unit leader follows the Institutional Data Access Request Procedure to submit the request to the appropriate Data Steward for approval.

3.8. Unit leaders monitor cleanup progress per training material.

3.9. The ISO runs periodic follow-up scans.

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

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, 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/infotech/Pages/Policies/Policies.aspx
- IT Procedure – Policy Development, Approval, and Implementation
- IT Reference – Common Definitions
- IT Policy – Institutional Data Access and Protection Policy
- IT Policy – Roles and Responsibilities for the Institutional Data Access and Protection Policy
- IT Procedure - Institutional Data Access Request Procedure

Contact Information

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