

Minimum Security Procedure for Handling Physical University Data

Summary

This document outlines the minimum security standards that are required for individuals who handle physical data (such as printed reports, letters, or memos) containing sensitive or internal University data. The purpose of these requirements is to reduce risks to the confidentiality and integrity of sensitive or internal University data (detailed in The University of Oregon Data Classification Policy) and to protect the privacy of members of the University community.

Scope

This standard applies to all individuals who handle physical data containing sensitive or internal University data.

Standard

Granting Access or Sharing

Access shall be limited to authorized University officials or agents with a legitimate academic or business interest on need to know basis.

Storage

If data needs to be retained while not being used or reviewed, the data must be stored in a locked device (such as a filing cabinet) and also be protected by a locked door when staff are not present.

Disclosure, Public Posting, etc.

Reasonable methods shall be used to ensure data is only disclosed to authorized individuals or individuals with a legitimate need to know. Sensitive data may not be posted publicly.

Printing, mailing, fax, etc.

Reasonable methods shall be used to ensure that printed materials are only distributed or available to authorized individuals or individuals with a legitimate need to know. Printed materials that include sensitive data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know. Access to any area where printed records with sensitive data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.

Disposal

When the data is no longer needed per records retention requirements, the paper should be shredded with a cross-cut shredder or destroyed by another appropriate method (such as a secured burn/destruction box).

Review of Procedure

This Procedure will be reviewed on an annual basis to implement, change, or remove controls based on altered security specifications and changes in laws, regulations, and best practices.

DRAFT