THE UNIVERSITY OF TENNESSEE
CHATTANOOGA

Security Guidelines for Handling Paper-based University Data

Summary

This document outlines the minimum security guidelines that are required for individuals who handle paper-based University data. The purpose of these requirements is to reduce risks to the confidentiality and integrity of sensitive University data and to protect the privacy of members of the University community.

Scope

This guideline applies to all users that handle paper-based sensitive University data.

Guideline

Granting Access or Sharing

Access to paper-based sensitive data shall be limited to authorized University officials or agents with a legitimate educational or business interest on a 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 and Public Posting

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

Access to any area where records sensitive and internal data are printed 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, and no longer required to be retained 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).