Minimum Security Procedure for Devices with Sensitive Information

Summary

This document outlines the minimum security procedures that are required for devices that store or process sensitive University data. The purpose of these requirements is to reduce risks to the confidentiality and integrity of sensitive 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 devices that store or process sensitive University data, including privately owned devices. Examples of these devices include servers, workstations, laptop computers, tablets, smart phones, printers, etc.

Standard

All devices that store or process sensitive data shall meet the following minimum security requirements.

Servers:

Physical security — Server class devices shall be placed within a protected and monitored area with a secure perimeter (e.g., walls, lockable doors and windows) that protects the system from unauthorized physical access.

Security updates — Devices shall be kept up-to-date with current operating system and third-party applications security patches and updates.

Anti-virus software — Anti-virus software shall be used and kept up-to-date if such software is available for the device.

Software firewall — Firewall software shall be used and kept up-to-date.

Limit network access — Network access to sensitive systems shall be restricted to the least access necessary for the device to perform its function/mission.

Access control — User accounts and users shall have a unique identifier (user ID/login name) that is assigned for their University business use only. Privileges shall be restricted and controlled in accordance with the principle of least privilege to reduce opportunities for unauthorized access or misuse of the system. Access and privileges shall be authorized by an appropriate authority and reviewed at regular intervals.

Secure login and authentication — Access shall be controlled with secure/encrypted log-on procedures.

Protection against brute force login attacks — Controls shall be put in place to limit failed login attempts.

Session controls — Controls shall be put in place to ensure that inactive sessions shall expire after a defined period of inactivity.

Logging and monitoring — System administrator and user activities and system events shall be logged. Logs shall be retained for a period of at least one year or a period deemed practicable by the University department/unit responsible for the security of the device, consistent with any applicable retention requirement.

Identification and management of vulnerabilities — Devices shall be hardened prior to implementation. Security updates shall be applied and unnecessary services disabled in order to minimize potential technical vulnerabilities.

Responsibility for security — Responsibility for the security of a sensitive server and its data shall be assigned to an individual.
Encrypted transmission of data — Encrypted protocols or secure channels shall be used to transmit sensitive data to and from the device.
Encrypted storage of data — Sensitive data should be stored in an encrypted state or have compensating controls to secure the data.

Desktops:
Physical security — Desktop devices shall be placed in reasonably secure areas such as lockable offices and not in publically assessable areas.
Login and authentication — Login or authentication procedures shall be used to prevent unauthorized logical access to devices.
Automatic security updates — Desktop devices shall be configured to automatically download and install security updates for operating systems and third-party applications whenever possible.
Anti-virus software — Anti-virus software shall be used and kept up-to-date.
Software firewall — Firewall software shall be used and kept up-to-date.
Auto-lock screens — Desktop devices shall be configured to automatically lock and require a logon after being unattended or inactive for a predefined period of time.
Least privilege for user accounts — User accounts shall be configured with the least privileges necessary for the users to perform their job/role.
Remove sensitive data when no longer needed — Devices shall be configured to automatically delete temporary files, temporary internet files, clear web browser caches, etc.
A process shall be adopted to regularly review archived files and delete files containing sensitive data when the files are no longer needed, consistent with applicable retention laws and regulations, or University policies.

Laptops, tablets, and mobile devices:
Physical security — Laptops (and where available/appropriate tablets and mobile devices) shall be protected from unauthorized physical access and theft by storing the device in a secure location, anchoring with a security cable, etc.
Login and authentication — Login or authentication procedures shall be used to prevent unauthorized logical access to devices.
Automatic security updates — Devices shall be configured to automatically download and install security updates for operating systems and third-party applications whenever possible.
Anti-virus software — Anti-virus software shall be used and kept up-to-date if such software is available for the device.
Software firewall — Firewall software shall be used and kept up-to-date if such software is available for the device.
Auto-lock — Devices shall be configured to automatically lock and require a logon, pin, or other means of authentication after being unattended or inactive for a predefined period of time.
Least privilege for user accounts — User accounts shall be configured with the least privileges necessary for the users to perform their job/role.

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 statutes, regulations, and best practices.