Minimum Security Procedure for Devices with Public or Internal Information

Summary

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

Standard

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

Security updates

Devices shall have all applicable security updates for operating systems and third-party applications installed as soon as practicable or, at a minimum, within 2 weeks of the security update release date.

Anti-virus software

Anti-virus software shall be used and kept up-to-date on devices where the use of such software is practical.

Software firewall

Firewall software shall be used and kept up-to-date on devices that have firewall software capabilities.

Access control

Devices shall require sign-on or login for users. Users shall be authenticated by means of passwords or by other authentication processes (e.g. biometrics or Smart Cards). In general, only encrypted authentication mechanisms or protocols shall be used.

Unnecessary services

Services that are not necessary for the device to perform its function or mission shall be disabled.

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.