OIT Minimum Security Standard for Desktop Systems

Table of Contents

1.0 Introduction

The purpose of this document is to outline a set of minimum security standards and best practices regarding desktop and end-user computer systems. The following standards are recognized throughout the IT industry to be "security best practices" and when adhered to are designed to enhance the overall integrity and availability of UA information resources, networks, and computer systems.

2.0 Scope

This document and the standards contained herein apply to all users, desktop computer systems, workstations, laptops and other end-user devices that are attached to University networks or are interacting with UA information resources managed by the Statewide (SW) and UAF Major Administrative Units (MAU).

3.0 Minimum Standard for Desktops

Software updates

Regularly check for and ensure that software updates/patches are installed. This includes, but is not limited to, operating system updates, application patches and firmware updates.

Anti-Virus Software

Install and maintain current anti-virus software. Check for and install any updates to both the software and virus definitions on a regular basis.

Implement Physical Security Measures

Workstations must be configured to require a password to access the system. Enable screen locking features to prevent unauthorized access to one's machine while not in use. Any exceptions such as public terminals, kiosks, or lab computers should be documented.

Disable Unnecessary Services

Many operating systems may be configured (by default) to permit access to ones system from other computers on a network. An assessment should be performed to identify all services enabled on a system. Any unnecessary services should be disabled and any exceptions (services left enabled due to business or operational requirements) documented.

Limit Use of Privileged Accounts

Under certain circumstances normal users may be issued system accounts that have administrative or privileged access to a system. Users should limit the use of these accounts (to the specific tasks requiring them) and not use them for general work purposes.

Host-based Firewall Software

Host-based firewalls help protect individual systems from malicious attacks initiated by other systems on a computer network. Workstations are required to have locally installed firewall software and have it configured in a secure manner approved by the UA Chief Security Officer.

4.0 Inquiries & Information

For more information, questions, and details regarding the above mentioned standards, please visit the OIT Security Administration website at the following link.

http://www.alaska.edu/itsecurity