USFSP Computing & Data Security Standards

Overview
The purpose of this standard is to identify a basic set of minimum standards for securing USFSP purchased computing devices and data. All USFSP purchased computing devices must adhere to this standard in addition to the USF System technology policies and standards. This standard may be more restrictive than USF System standards, but is not less restrictive. While this standard may restate portions of USF System policies and procedures it is important to read the related USF System policies and standards in addition to this document.

Laptop/Tablet Encryption
According to the Information Technology Management Council (ITMC), all laptops purchased by the University must have approved whole disk encryption software installed (ISSP-012).

In support of USF System standard ISSP-012, laptops with MS Windows installed must have a Trusted Platform Module (TPM) chip to allow for BitLocker whole disk encryption. Per USFSP standards, Mac devices must use FileVault to encrypt the hard drive.

Campus Computing will not disable laptop/table encryption for users traveling, regardless of the requirements imposed by foreign countries. Users are responsible for knowing and understanding the laws and regulations for technology of the foreign countries they are traveling to. It is also the user's responsibility to understand the export control rules while traveling overseas. They should review the information provided through USF Research and Innovation prior to traveling with technology.

Securing Centrally Managed Devices
Campus Computing centrally manages and secures university purchased Windows devices using a variety of management and security tools. Non-Windows devices are individually managed and secured. *Update: Campus Computing is currently investigating ways to centrally manage and secure Apple devices.*

- **Group Policies** are used to define and enforce standard computer configurations to provide a standardized layer of security across all domain joined devices.
- **Windows Update** is enabled to allow Windows and Microsoft Office updates to be installed on university computers.
- **Lumension Deployment Manager** uses an agent installed on university devices to deploy or remotely install security and application updates for common applications.
- **Microsoft System Center Configuration Manager** uses an agent installed on university devices to deploy full applications, Operating Systems, and updates.
- **Cisco AMP for Endpoints** provides protection against advanced malware attacks.
- **Trend Micro** provides antivirus protection for university devices. *Note: Unlike the previously used antivirus solution (Symantec), Trend Micro is not available for personal devices. Please visit*

the USF Antivirus Protection website for more information and recommendations. The products listed are not supported by USF Tampa IT or USFSP Campus Computing

Related USF System Policies and Standards

Policies

- ISSP 0-501 (IT Security) - Using and Protecting Microcomputing Resources
- ISSP 0-502 (IT Security) - Appropriate Use of Information Technology Resources
- ISSP 0-515 (IT Security) - Protection of Electronic Personal Information
- ISSP 0-516 (IT Security) - USFID-SSN Appropriate Use Policy
- ISSP 0-507 (IT Governance) - Data Management

Standards

- ISSP-001 - Sensitivity and Criticality of Data
- ISSP-005 - Choosing Strong Passwords
- ISSP-006 - Securing Sensitive Computers
- ISSP-009 - Electronic Data and Media Disposal
- ISSP-012 - Data Protection Standards for Mobile Devices
- ISSP-013 - Request for Storage of PII on a Mobile Device
- ISSP-014 - Request for Storage of Social Security Numbers