Practice Directive Title: Workstation Management DRAFT

Division: Administration and Finance
Department: Information Technology Services
Contact Information: Chief Information Officer / Nish Malik / 415/338-1133 / nish@sfsu.edu
Effective Date: September 4, 2018
Revised Date: September 4, 2018

Authority:

Integrated CSU Administrative Manual 8000 Information Security

8045.S400	Mobile Device Management Standard
8050	Configuration Management
8050.S01	Common Workstation Standard
8050.S02	High Risk Workstation Standard
8060	Access Control
8065	Information Asset Management
8075	Information Security Incident Management
8105	Responsible Use Policy

San Francisco State University Practice Directives

- SF State Mobile Device Practice Directive
- SF State Active Directory Practice Directive
- SF State Password Practice Directive
- SF State Secure E-Waste and Paper Disposal

Objective:

The Workstation Management Practice Directive defines the maintenance and configuration requirements for the management of university and auxiliary-owned workstations. Common and high-risk workstation standards must be followed. Campus IT support providers must be able to track information technology assets and remediate endpoint vulnerabilities to manage risk.

Definitions:

Workstations: Refers to desktop, laptop (notebook), and devices running supported workstation operating systems including secondary or virtualized supported workstation operating systems. Any workstation on the campus network is in scope for compliance with this directive even if no longer in use for its intended purpose.

Common Workstations: Refers to the configuration and state of workstations as described in ICSUAM 8050.S01.

High-Risk Workstations: Refers to the configuration and state of workstations as described in ICSUAM 8050.S02.

Statement:

The Workstation Management Practice Directive covers all University-owned workstations used to access or store SF State data including Mac and Windows-based desktops and laptops. Workstation management may be conducted manually or using an automated tool according to timelines and criticalities established in workstation security guidelines. The following guidelines must be followed for workstation management:

Workstation Reporting

- Enable data gathering for hardware, operating system, applications and configuration running on workstations
- Follow active directory and DNS naming conventions to associate devices with user, location, and support area
- Track all devices storing confidential level 1 data

Patch Management

- Deploy operating system and application updates and patches to remediate vulnerabilities

Operating System Deployment

- Deploy operating systems that adhere to common or high-risk workstation standards

Application Deployment

- Install, un-install and configure applications

Data Security

- All non-public workstations must be encrypted
    - Computer lab workstations may be reviewed on a case-by-case based on usage

Configuration Management

- Minimum configuration settings must be included in all deployments

Workstation Management Tool Administration

- Workstation management tools must use the approved campus Active Directory service for authentication and authorization
- Hosting for tools used for the management of high-risk workstations must meet the requirements of a high-risk workstation

Decommissioning and Disposal

- Workstations no longer in use and ready for removal from the campus environment must follow secure e-waste and property control procedures

Implementation:

Responsibility for implementing this practice directive will rest with Information Technology (IT) units across campus. Submit any apparent violation to the appropriate administrative authority (vice president, dean, director, department, or program chair) or to service@sfsu.edu. Any exceptions to this practice

directive must be documented using a risk assessment and approved by a Vice President, the Chief Information Officer and Information Security Officer.

Non-Compliance:

Noncompliance with applicable policies and/or practices may result in suspension of network and systems access privileges. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements.

Searchable Words:

Endpoint, workstation, manage, configuration, deployment, update, patch, maintain