Standard: Workstation Hardware

Information Security Standards

Workstation Hardware

Standard #	IS-WH	Effective Date	2/15/16	Email	security@sjsu.edu
Version	3.0	Contact	Mike Cook	Phone	408-924-1705

Revision History

Date	Action
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.
2/13/2016	Updates per Academic Affairs input. – Mike Cook
1/13/17	Added encryption and administrative privileges. – Hien Huynh

Table of Contents

Introduction and Purpose

This standard outlines the minimum specifications required for the purchase of Workstation hardware. For the purpose of this document, a Workstation is defined as any Desktop, VDI Thin Client, Laptop, or Mobile Tablet type device.

This standard is not intended to be a complete specification of system requirements, but rather highlight the required elements Workstation configurations.

Scope

This standard applies to all workstations purchased by operational-fund, self-support, and auxiliary units of the University.

Workstation Hardware Standard

All Workstation purchases handled by the University Purchasing Office shall be directed through the IT Services, Workstation Refresh Program.

Configuration

PC Computers

PC's purchased for all purposes should be enterprise models (i.e Dell Optiplex) rather than consumer models (i.e. Dell Inspiron). Workstations shall not be assembled from individual components for the purposes of University business.
Required elements for PC purchases are as follows:

- Capable of running the latest release of the Microsoft Windows Operating System
- Implement the latest versions of campus Antivirus/Antimalware software, patch management software, and vulnerability management software.
- Computers storing confidential (Level 1 and Level 2) must support Trusted Platform Module (TPM 2.0 or higher)
- 8GB of ram or higher
- Dual-Core Intel i3 or higher processor, Intel Core2Duo 1.2Ghz or better
- 128GB or larger hard/flash drive
- 10/100/1000 Network Card
- Optional Wireless cards must support 802.1x Wireless Network access via WPA2 Enterprise encryption
- Must support Audio output and Video output

Apple Computers

Required elements for Apple purchases are as follows:

- Capable of running the latest release of the OSX Operating System
- Implement the latest versions of campus Antivirus/Antimalware software, patch management software, and vulnerability management software.
- 8GB of ram or higher
- Dual-Core or higher processor, Intel Core2Duo 1.2Ghz or better
- 128GB or larger hard/flash drive
- Optional Wireless cards must support 802.1x Wireless Network access via WPA2 Enterprise encryption
- Must support Audio output and Video input

VDI Thin Clients

Required elements for VDI Thin Client purchases are as follows:

- Must support PC Over IP
- Must be purchased along with Microsoft Windows VDA License
- Must support at least 2 monitors
- Minimum 512MB On-Board Memory

Laptops

Laptop computers require approval from Department Management. Laptops must follow the requirements for PC/Apple Computers.
Additional required elements for Laptop purchases are as follows:

- PC's must support Trusted Platform Module (TPM 2.0)
- Wi-Fi Wireless Networking Card which supports 802.1x Wireless Network access via WPA2 Enterprise encryption

Mobile Tablets

Additional required elements for Tablet purchases are as follows:

- Must be compatible with current IT Services Mobile Device Management software and standards. (Contact IT Services for more information)
- Must store all data on the device encrypted when not in use
- Must support 802.1x Wireless Network access via WPA2 Enterprise encryption
- Must support complex passwords (> 4 characters)
- Must support remote tracking and wiping (I.E. Find my iPad)

Asset Management

Per ICSUAM 8065.0 SJSU is responsible for maintaining an inventory of information assets containing level 1 or level 2 data (University Technology Asset Inventory). Due to the widespread availability of sensitive data (passwords, health insurance information, medical records, home addresses, library circulation information, bids, facilities diagrams, grades, student data, etc.) all workstations must be tracked. Separate from University Property Office procedures, all Department Information Technology teams will create a record for and assign an IT Services or University Property Office issued property tag for each device capable of storing sensitive data. No device capable of storing sensitive information shall be used without proper identification and asset management.

Upon delivery of the device, the receiving department shall assume responsibility for the tracking of the information asset. Per ICSUAM 8065.0, departments must be able to report on current location, current owner, data disposition status, and survey status.

Each device will be reviewed once every year as part of the campus anti-theft program. Each device will be replaced every four years as part of the campus refresh/recycle/survey process. Each department will receive a Physical Inventory Discrepancy memo noting any missing equipment. Each department will be given 10 days to locate the property. If the department is still unable to locate the property after the 10-day grace period, the department will note that the property is missing on a Missing Equipment Report which will be forwarded to the San Jose State Police Department for investigation.

Definitions

Workstation

Any Desktop computer, VDI Thin Client, Laptop Computer, or Mobile Tablet type device.

Desktop
A personal computer small enough to fit in an individual workspace. Does not have to be capable of storing data.

Examples:
- Acer Aspire
- Apple Mac Mini, iMac, and Mac Pro
- Asus E-Box and Essentio
- Dell Alienware, Dimension, Optiplex, Precision and XPS
- Gateway SX Series
- HP Pavilion, 110, and Compaq
- Lenovo Erazer, C, H and K Series
- Sony VAIO

VDI Thin Client
A personal computer small enough to fit in an individual workspace incapable of standalone operation, and capable of "virtually" performing Desktop activities on a centralized server. These devices are essentially terminal devices which provide keyboard, USB, and mouse inputs and audio/video outputs to the user.

Examples:
- Acer Veriton
- Dell C, D, R, T, V, Z Series and Wyse
- HP MultiSeat, T Series, and Smart Client

Laptop
A personal computer that is portable. Does not have to be capable of storing data. Includes Touchscreen and Traditional Screen Tablets, and Convertible devices which are capable of running a Desktop Operating System (i.e. Microsoft Windows, Apple OSX)

Examples:
- Acer Aspire
- Asus VivoBook
- Apple MacBook and MacBook Air
- Dell Alieneware, Inspiron, Latitude, Precision, NB, Slate (ST), Venue (Windows Models) and XPS
- HP Envy, Pavilio, and Split
- Google Chromebook
- Lenovo Ideapad and Yoga
- Samsung ATIV
- Sony VAIO
- Toshiba Satellite

Mobile Tablet
A personal computing device that is portable. Does not have to be capable of storing data. Includes Touchschreen and Traditional Screen devices, Tablets, and Readers which run on a

device-specific mobile operating system (i.e. Apple iOS, Android, Nook, Kindle). Does not include Cellular Phones

Examples:

- Acer Iconia
- Amazon Kindle and Kindle Fire
- Apple iPad, iPad Mini, and iPod
- Asus MemoTab, VioTab, and Transformer
- Barnes and Noble Nook
- BlackBerry Playbook
- Dell Venue (Android Models)
- Google Nexus
- HP Slate and Split
- Microsoft Surface and Surface Pro
- Samsung Galaxy
- Sony Xperia

Data Encryption

All SJSU computers including desktops, laptops, tablets, mobile devices and server storing level one data must implement an ISO approved data encryption tool. SJSU users cannot encrypt their own computers, encryption needs to be implemented by their Department Technician. Users shall not knowingly take actions which prevent campus technicians from accessing University computers. For more information on Data Classifications, please refer to the Information Classification and Handling standard.

Administrative Privileges

Administrative privileges are the highest level of permission that can be granted to a computer user, and with this permission comes a higher level of responsibility. Levels of permissions are necessary in networked environments to ensure system security and prevent damage to computer hardware and software. A user with administrative privileges can perform tasks such as install and uninstall software and change a computer's configurations. A user with administrator privileges must be aware s/he will have access to confidential, personal information, control panels, registry settings and other components that could irreparably harm their system. The user may access only those functions necessary to complete his/her task. For more information on administrative privileges please refer to the Access Control Standard. For request for workstation administrative privileges, please fill out the Request for Workstation Administrative Privileges form.

Information Security

This standard is not intended to replace any pre-existing SJSU, CSU, local, state, or federal law, standard policy or practice. All Workstations purchased shall abide by all applicable information security policies.

Standard Management

In accordance with CSU policies, the San José State University Director of Desktop Support Services oversees an annual review of this Standard and communicates any changes or additions to appropriate SJSU stakeholders. The SJSU Workstation Hardware Standard shall be updated as necessary to reflect changes in CSU policies, SJSU's academic, administrative, or technical environments, or applicable laws and regulations. The Information Technology Management Advisory committee shall perform a bi-annual review of this standard.

The standard may be augmented, but neither supplanted nor diminished, by additional policies and standards.