1.0 Introduction

This standard outlines the minimum specifications required for Workstation Security. 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. Related configuration standards include:

- 8050.S100 Configuration Management – Common Workstation Standard
- 8050.S200 Configuration Management – High Risk Workstation Standard
- 8050.S300 Configuration Management – Mobile Device Standard
- 8045.S600 Information Technology Management - Logging Elements

This standard describes the minimum requirements the campus has identified to secure systems to acceptable risk levels

Implements: ICSUAM 8050.0 Configuration Management


2.0 Scope

This standard applies to all workstation devices or instances administered by Sacramento State, any of its auxiliaries, or connected to or hosted by the Sacramento State network.

3.0 Asset Management

Per ICSUAM 8065.0 Sacramento State is responsible for maintaining an inventory of information assets containing level 1 or level 2 data (University Technology Asset Inventory). Due to the widespread use 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 must 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 Sacramento State Police Department for investigation.

4.0 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, currently Bitlocker. Sacramento State 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. be reported to the appropriate team for investigation.

5.0 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

6.0 High Risk Workstation

From CSU 8050.S200 Configuration Management – High Risk Workstation Standard

5.0 Definitions
Server – A combination of hardware, operating system, network service, application software, and network connection that provides a function. Server description can include, but is not necessarily restricted to the following:

- Uses a client-server architecture
- Has the ability to manage files, services and other networked resources
- Provides authorized clients with access to files, services and other networked resources
- Is operationally bound to the applications it hosts
- Has the ability to handle multiple connections and requests
- Can be using hardware or software based virtualization technology

High-risk Server - Any server that stores or processes “critical” data or systems. A server may be designated as “high risk” based on a combination of factors, including but not limited to:

- The storage or processing of protected level 1 information in such quantities as to require notification of a government entity (i.e. over 500 records under HIPAA or CA 1798.29), or information classified as protected level 1 due to severe risk.
- Serving a critical function requiring very high availability (i.e. the emergency notification system, or campus firewall)

Information Security Officer (ISO) or Chief Information Security Officer (CISO) – See ICSUAM 8015.S000 “Information Security Roles & Responsibilities”

Information Security Analyst/Administrator – A campus employee or consultant who:

- provides information to server administrators on best practices to secure servers
- conducts vulnerability assessments prior to servers being deployed
- assists with or performs the risk assessment activity for servers

Personal Identifiable Information – ICSUAM 8065 - Data Classification Standard defines this as Protected Level 1 Data.

Primary Server Administrator – Primary contact for a particular server. Ensures that all existing and new servers are configured to support the minimum standards, or that an alternate plan for risk management is provided. Primary Server Administrators are also responsible for requesting vulnerability assessments for new servers and mitigating found vulnerabilities.

Application Owner – the individual or group with the responsibility to ensure that the program or programs, which make up the application, accomplish the specified objective or set of user requirements.
**Risk Owner** - The individual or group who is ultimately accountable for ensuring the risk is managed appropriately, approving such compensating controls as determined necessary.

**IaaS** – A cloud environment offering infrastructure as a service. The campus is able to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

**PaaS** – A cloud environment offering platform as a service the is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming

### 7.0 Documentation Review and Approval

Review/Approval History

<table>
<thead>
<tr>
<th>Date</th>
<th>Audience</th>
<th>Action</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>