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 of Workstation configuration. Related configuration standards include:

- CSU Common Workstation Standard
- CSU High Risk/Critical Workstation Standard
- Mobile Device Management
- ISO Domain 18: Compliance Standard: Exceptions
- Information Asset Monitoring: Logging Elements

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

Implements: CSU Information Security Policy: ISO Domain 12: Operations Security Policy Policy Reference: https://calstate.policystat.com/policy/11773867/latest/#autoid-wj683 Standard Reference: https://calstate.policystat.com/policy/11773867/latest/#autoid-6w2ve

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 Sacramento State Implementation of the Common Workstation Standard

Minimum Configuration Features	MAC	Windows
Password Management: State owned desktop and laptop computers must comply with the campus password complexity and aging policies.	Computer joined to the CSUS domain and uses a SacLink account in AD with password policy enforced	Computer joined to the CSUS domain and uses a SacLink account in AD with password policy enforced
Inventory	Property Management (WASP) and JAMF Cloud	Property Management (WASP) and SCCM
Campus method for managing computer inventory records	Property Management (WASP) and JAMF Cloud	Property Management (WASP) and SCCM
All desktop and laptop computers purchased by the University must be tracked via the campus inventory management system	Property Management (WASP) and JAMF Cloud	Property Management (WASP) and SCCM
The campus must establish a periodic inventory process to ensure that inventory records are current and accurate, and contain information sufficient to support data classification and incident response activities	Property Management (WASP) and JAMF Cloud	Property Management (WASP) and SCCM
All workstations must be encrypted using campus approved encryption method and tracked and managed via the campus inventory process. Workstations running DeepFreeze are exempted from the encryption requirement.	Jamf Cloud managed Recovery Lock (all Apple Silicon based Macs)	MBAM managed BitLocker

Peripherals, external drives and memory sticks, which store Level 1 protected data must: **i.)** Be encrypted using campus approved encryption methods. **ii.)** Be tracked and managed via the campus inventory process.	External Drives & memory sticks need to be purchased with an encryption technology on the device (list of approved devices available from IRT)	External Drives & memory sticks need to be purchased with an encryption technology on the device (list of approved devices available from IRT)
Anti-Virus: Up to date anti-virus software must be installed and maintained on all systems. Regular updates to virus definitions and software must be activated.	Campus managed MalwareBytes	Campus managed Microsoft Defender
Software Updates: Workstation computers must be configured to allow automatic application of software updates through a patch management system.	Jamf Cloud	SCCM and Patch My PC
Supported Operating systems: The desktop or laptop device must use a supported operating system in order to ensure that security vulnerabilities are addressed. Where the campus determines that an exception to this standard applies, the campus exception documentation must include controls sufficient to address the risk.	Supported OS list: https://support.apple.com/en-us/HT201222 - Campus exception process in place for requested exceptions	Supported OS List: https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet - Campus exception process in place for requested exceptions
Enterprise Management: The workstation must be managed by an appropriate configuration management system, such as a campus enterprise desktop management system, that ensures: a) The workstation is subject to periodic vulnerability reporting. b) The success and/or failure of critical patches is reported.	JAMF Cloud and Qualys VMDR	SCCM and Qualys VMDR

Inactivity Screen Lock	See Below	See Below
a) Workstations must be configured with screen locking features to prevent unauthorized access to a machine while not in use.	JAMF Cloud configuration profile 30 minutes for common workstations, 15 minutes for high-risk workstations, 60 minutes for instructional machines in classrooms and labs	GPO 30 minutes for common workstations, 15 minutes for high-risk workstations, 60 minutes for instructional machines in classrooms and labs
b) Campuses must identify screen lock time limits appropriate to the purpose of the workstation and the environment in which it is located.	JAMF Cloud configuration profile 30 minutes for common workstations, 15 minutes for high-risk workstations, 60 minutes for instructional machines in classrooms and labs	GPO 30 minutes for common workstations, 15 minutes for high-risk workstations, 60 minutes for instructional machines in classrooms and labs

4.0 Tools Definitions

BitLocker – Hard drive encryption tool for Windows computers

FileVault – Hard drive encryption tool for Macs

GPO – Microsoft's Group Policy Object used to configure settings for large groups of computers

Jamf Cloud – Common campus infrastructure used to centrally maintain an inventory of campus Macs, deploy software, and deploy configurations.

Microsoft Defender – Anti-virus and endpoint protection

SCCM – Microsoft System Center Configuration Manager – Common campus infrastructure used to centrally maintain an inventory of campus workstations, deploy software, and deploy configurations.

WASP – Inventory management software maintained by Facilities Management

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
8/11/2020	IT Collaboration and Standards Group Meeting	Draft presented to campus IT personnel in the meeting and feedback solicited.
10/14/2020	IRT Staff and Management	Draft updated based on campus IT personnel feedback.
11/4/2020	IT Collaboration and Standards Group Meeting	Updated draft reviewed.

11/24/2020	IRT Staff and Management	Draft reviewed and outstanding items plan drafted.
8/11/2020	IT Collaboration and Standards Group Meeting	Draft presented to campus IT personnel in the and feedback solicited.
12/1/2020	ISO	Draft published for campus.
12/4/2020	IRT Staff and Management	Draft updated.
12/9/2020	IRT Staff and Management	Draft updated.
2/25/2021	IRT Staff and Management	Draft updated.
3/1/2021	IRT, Director of Policy and Records Management	Recommended for approval/publication.
3/8/2021	Cabinet	Approved.
10/13/2021	Change Control	Updates approved.
12/1/2021	Change Control	Updates approved.
11/16/2022	IT Collaboration and Standards Governance Meeting	Updates presented.
11/16/2022	Change Control	Updates approved.