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-zk3v3

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 Definitions

A “High Risk” workstation is defined as any workstation that stores or accesses “critical” data or systems. “Critical data” includes 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. “Access to critical systems” means an elevated access privilege to a system which stores protected level 1 information. Examples of this may include access to the Student Health System, access to payment card processing system, access to student financial records, etc.

4.0 Sacramento State Implementation of the High Risk Workstation Standard

Minimum Configuration Features	MAC	Windows
High Risk Governance		
Incorporating Common Workstation Standards	All High Risk Workstations must meet Common Workstation Standard. See Sacramento State's Common Workstation Standard.	All High Risk Workstations must meet Common Workstation Standards. See Sacramento State's Common Workstation Standard.
High Risk Workstation Designation: Campuses must implement a process for designating and reviewing the designation of critical or high risk workstations.	Identification and review of high-risk workstations is part of the campus annual security review and biennial sensitive data inventory survey. The ongoing process is available at: KB0011772	Identification and review of high-risk workstations is part of the campus annual security review and biennial sensitive data inventory survey. The ongoing process is available at: KB0011772
Change Control: The configuration of a High Risk Workstation may not be altered except as approved via the campus Change Control Process.	Changes must be referred to campus Change Control	Changes must be referred to campus Change Control
Physical Security: High Risk workstations must be physically protected as per the CSU Information Security Policy - ISO Domain 11: Physical and Environmental Security Policy.	Physical security standards must meet CSU Physical and Environmental Security Standard.	Physical security standards must meet CSU Physical and Environmental Security Standard.
High Risk Workstation Configuration		
Network Protection: In order to protect the high risk workstation from malware and/or data exfiltration, network access must be limited. Additional network protection can be achieved by **one or more of the following** methods, to be determined by risk assessment.	Cortex XDR and PAN URL filtering	Cortex XDR and PAN URL filtering

Network traffic limited to the minimum necessary to perform business functions by use of isolated network segment with traffic restricted to authorized inbound and outbound ports and destinations. (Please note that this may be used in combination with a virtual desktop environment for other work functions (web browsing, etc. to address productivity.)	PAN URL filtering	PAN URL filtering
Intrusion detection and prevention technologies which address hostile sites, malware, etc.	MalwareBytes	Windows Defender
Software defined networking, user based and/or application-defined routing or similar use of technology to control connectivity.	PAN URL filtering MalwareBytes	PAN URL filtering Windows Defender
Protection Against "zero day" Malware: For high risk workstations with operating systems commonly vulnerable to malware, either restricted outbound network egress or application whitelisting must be used in order to protect against “zero-day” malware.	Cortex XDR/PAN	Cortex XDR/PAN
Host-based Firewall: In order to prevent unauthorized access from other “local” hosts, a Host-Based Firewall must be enabled and configured to restrict access to only authorized hosts.	Mac OS Firewall	Windows Defender Firewall
Security Event Logging		
The High Risk Workstation must be configured to log security events.	Macs are set up to create local logs.	Local event logs in Windows event collector. Transported to LogRhythm.
Campus must identity the logging requirements and configuration settings for the	Logs are kept locally for 30 days.	Logs are forwarded to LogRhythm.

high risk workstation and its application environment including: i. Remote or local log storage ii. Log retention of at minimum 30 days		
Log activity must comply with CSU Information Security Policy – Information Asset Monitoring (Logging Elements)	Refer to CSU Information Security Policy – Information Asset Monitoring (Logging Elements) for logging elements.	Refer to CSU Information Security Policy – Information Asset Monitoring (Logging Elements) for logging elements.
Administrative Accounts: Local administration rights must not be granted to the campus account used for activities such as web browsing. As necessary, the user may be issued a separate local administration account.	No Admin Permissions granted. A separate account that is not used to log into the workstation can be requested via a risk exception request if administrative access is necessary.	No Admin Permissions granted. A separate account that is not used to log into the workstation can be requested via a risk exception request if administrative access is necessary.
Encryption: High Risk Workstations must use University approved encryption on both the hard drive and removable device peripherals and/or media.	Recovery Lock (all Apple Silicon based Macs) FileVault (all Intel based Macs)	BitLocker
Remote Support: Remote support applications must be configured to require the user to acknowledge and consent to the remote session.	Zoom/Teams	SCCM/Zoom/Teams
High Security Workstation Configuration Checklists: High Risk Workstations must use a current standard secure configuration checklist. Useful resources for developing a checklist include but are not limited to those offered by CIS benchmarks, National Institute of Standards and Technology (NIST USCGB) and/or the Department of Homeland Security.	CIS Benchmarks for MacOS	Microsoft Security Baseline
Vulnerability Scanning: Periodic vulnerability scans must be completed and	Qualys VMDR	Qualys VMDR

assessed in order to verify that operating systems and application are adequately updated (see CSU Information Security Policy – ISO Domain 12: Operations Security Standard - Configuration Management).		
Peripheral Communications: Peripherals and association communication protocols (e.g. Bluetooth) must either be adequately secured via encryption or disabled in order to avoid unauthorized access and denial of service issues.	Recommend disabling peripheral and association protocols to address the vulnerability and inconsistency with device encryption	Recommend disabling peripheral and association protocols to address the vulnerability and inconsistency with device encryption

5.0 Tools Definitions

Cortex XDR – Cortex Extended Detection Response - Endpoint and cloud threat detection tool

BitLocker – Hard drive encryption tool for Windows computers

FileVault – Hard drive encryption tool for Macs

Firewall – Personal/endpoint firewall tool built into Macs to detect incoming and outgoing network traffic to assist in blocking unnecessary or malicious traffic

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

LogRhythm – Computer and network log collection and analysis tool

Microsoft Defender – Anti-virus and end point protection

PAN – Campus firewall tool to detect incoming and outgoing network traffic to assist in blocking unnecessary or malicious traffic

Qualys – Security vulnerability and web application scanner

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

Windows Defender Firewall – Personal/endpoint firewall tool built into Windows computers to detect incoming and outgoing network traffic to assist in blocking unnecessary or malicious traffic

Zoom – Video conferencing tool with built-in workstation remote control capability

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 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.
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.
11/16/2022	IT Collaboration and Standards Group Meeting	Updates presented
11/16/2022	Change Control	Updates approved
11/30/2022	IT Collaboration and Standards Group Meeting	Updates presented
11/30/2022	Change Control	Updates approved