1.0 Introduction

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

A vulnerability is a weakness or flaw in software which may be used to compromise or undermine the system upon which it is located. Vulnerability management involves the identification, classification, remediation, and mitigation of vulnerabilities which are found in workstation operating systems, programs, and applications. Vulnerabilities pose a risk to the confidentiality, integrity and availability of University resources, as well as those whose data is stored by the University, or others that access University systems. To reduce this risk, vulnerabilities must be identified and remediated in a timely manner. This standard describes the minimum requirements the campus has identified to secure systems to acceptable risk levels.

In general, patches that address vulnerabilities should be applied as pervasively and as timely as possible.

Supplement Standard to: Sacramento State Vulnerability Management Standard

Standard Reference:

https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-vulnerabilitymanagementstandard.pdf

2.0 Scope

This standard applies to all workstation devices or instances managed by Sacramento State, any of its auxiliaries, or connected to or hosted by the Sacramento State network. This standard does not apply to personal devices connected to the wireless network or the Residence Hall VLAN.

3.0 Roles and Responsibilities

Information Security Office (ISO)

- Develop and maintain vulnerability management standards and supplemental workstation security standards.
- Monitor compliance.

- Identify non-compliant systems and contact system owners and business area administrators prior to removal from campus network except by critical need.
- Manage the removal of non-compliant systems or applications from campus network and/or block and segment.
- Document security exceptions for non-compliant systems where risk will be accepted.
- Coordinate communication for out of band/emergency patching.

Assigned Desktop Support Personnel

Assigned Desktop Support personnel can be either local IT support or Information Resources & Technology personnel as determined by the IT support structure of the department, college, or program.

- Add Windows and Mac workstations to campus managed workstation environments (SCCM or Jamf Cloud).
- Configure workstation management environment and 3rd party patching environment to monitor Windows and Mac workstations.
- Configure Windows and Mac workstation management environment and 3rd party patching environment to patch workstations within the required mitigation and patching schedule.
- Add necessary agents to Windows and Mac workstations to be managed by the workstation management environment and the 3rd party patching environment.
- Add campus supported vulnerability scanning agents to Windows and Mac workstations
- Configure campus managed workstation environments and 3rd party patching environment to implement the required mitigation and patching schedule.
- Mitigate high severity vulnerabilities within the required mitigation and patching schedule.
- Review patch reports to ensure workstations are being patched within the required mitigation and patching schedule.
- Ensure the campus approved Anti-virus product is installed, running, and kept updated on the workstations.
- Perform required out of band/emergency patching.

Workstation Owners

A workstation owner is defined as the individual who has been assigned the campus workstation or is the primary user of the workstation.

- Patching should be allowed as soon as it does not interfere with academic or business needs.
- The patching effort must not be hampered by making changes to the workstation or disabling the network connection.
- When required, computer reboots must be allowed.

4.0 Supplemental Standards for Workstations

4.1 Required Vulnerability Management

Workstation operating system, software, and application vulnerabilities must be scanned/monitored/registered in accordance with campus vulnerability management requirements.

Noncompliant devices and those devices which represent a risk to the confidentiality, integrity, and availability of campus information assets are subject to removal from the campus network and quarantine.

4.2 Enrollment in Campus Managed Workstation Environment

While there are numerous tools that can provide insight into the vulnerabilities on a system, not all tools have the same set of features, Sacramento State has implemented workstation management tools for Windows and Macs. Use of any other management environment requires a security risk exception and must be approved by the Information Security Officer. The campus management tool for Windows is SCCM and the management tool for Macs is Jamf Cloud.

4.3 Enrollment in 3rd Party Patching Management Environment

While there are numerous tools that can provide 3rd party patching of applications, not all tools tools have the same set of features, Sacramento State has implemented a 3rd party patching tool for Windows and Mac workstations. Use of any other 3rd party patching tool as the primary patching tool requires a security risk exception and must be approved by the Information Security Officer. The campus 3rd Party Patching Management tool for Windows is Patch My PC. The campus 3rd Party Patching Management tool for Macs is Jamf Cloud. If there are patching tools that the campus 3rd Party Patching Management tool do not address, that product may be used in addition to the campus 3rd Party Patching Management tool.

4.4 Vulnerabilities Not Addressed by Workstation Management Environment and 3rd Party Patching Tool

There may be some vulnerabilities that are not identified by either the management environment or 3rd party patching tool. Additionally, there may be vulnerabilities that either the management environment or 3rd party patching tool cannot patch. If there is a vulnerability identified by other means and it can be patched by means other than the managed environment or via the 3rd party tool, it still must be patched if it meets the established threshold and it is not unreasonable to patch (e.g., cost prohibitive or is technically unfeasible). If it is decided that this vulnerability should not or cannot be patched, the risk must be reported to the Information Security Office and documented as a security risk exception.

4.5 Workstation Deployment

Before a workstation is added to the campus network, known vulnerabilities that meet the established threshold must be mitigated.

This can be accomplished by imaging a machine on the campus network if the machines are patched as they are imaged.

Alternatively, the workstation can be attached to a segmented VLAN (e.g., equipment VLAN) that cannot be accessed via the internet or by the campus at large. The VLAN should be configured to only allow workstation access to sites/destinations necessary to complete the required patching.

This practice must be used for workstations that have been off the network and left unpatched for six months or have a vulnerability with a known active exploit that is affecting the campus.

Additionally, the managed workstation environments should be configured to automatically patch managed machines that come onto the network if they have not been patched for six months and start the timer for an automatic restart.

4.6 Check-In Frequency

All actively used campus workstations must check-in with the workstation management environment and the 3rd party patching tool at least once a week.

4.7 Vulnerability Threshold

All critical OS vulnerabilities as identified by a respective vendor must be remediated in accordance with the mitigation and patching schedule and/or out of band/emergency patching criteria.

Applications with a vulnerability score of 6 or greater using the Common Vulnerability Scoring System (CVSS) or with a high (or equivalent) rating by the vendor or with the Patch My PC scoring of Security Critical must be remediated in accordance with the mitigation and patching schedule and/or out of band/emergency patching criteria.

OS and application vulnerabilities identified by the Information Security Office (ISO) with a risk exposure mapping value of critical or high using the Risk Exposure Mapping table below or as urgent or critical based on the Qualys severity scale that follows must be remediated in accordance with the mitigation and patching schedule and/or out of band/emergency patching criteria. If not already scored, the ISO will score the severity of the vulnerability based on equivalent reported scales, information provided by vendors, professional associations, or university community colleagues (e.g. Dell Secureworks, REN-ISAC, CSU Chancellor's Office).

Vulnerabilities below the threshold established above, should be mitigated when possible and after the above threshold has been prioritized. Vulnerabilities below this threshold will not be enforced unless there is an active exploit that could pose a risk to confidentiality, integrity, or availability.

Risk Exposure Mapping Values

Risk Exposure Mapping

		Severity			
		Critical	High	Moderate	Low
Likelihood	Very High	Critical	Critical	High	Moderate
	High	Critical	Critical	High	Low
	Moderate	High	High	Moderate	Low
	Low	Moderate	Moderate	Low	Low
	Negligible	Low	Low	Low	Low

Qualys Severity Scale

Urgent - Severity 5 Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Critical - Severity 4 Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.

Serious - Severity 3 Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

Medium - Severity 2 Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

Minimal - Severity 1 Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

Note: Vulnerability severity levels listed above were defined by Qualys Inc.
https://qualysguard.qualys.com/qwebhelp/fo_help/knowledgebase/vulnerability_levels.htm

4.8 Vulnerability Mitigation and Patching Schedule

Patchable Vulnerabilities meeting the vulnerability threshold must be addressed within 30 calendar days from detection with an additional allowance of 14 days for testing the patches if desired. The default schedule for implementing the patching can be set to 44 days to accommodate consistent testing of patches. The implementation should remain at 30 days if testing will not be regularly applied.

4.9 Out of Band/Emergency Patching

There may be occasions when a vulnerability poses a significant and immediate threat to either confidentiality, integrity or availability of university information assets. At the discretion of the Information Security Officer or Chief Information Officer and with notice to the Office of the President, a patch may be required to be applied despite the risk to academic or work interruption. Campus IT personnel may be asked to immediately apply a patch, or when available, a patch may be immediately applied to all managed campus machines by Information Resources & Technology personnel. This may include workstations, applications, or vulnerabilities that have been granted an exception.

4.10 Enforcement

Workstations not remediated within the required remediation schedule or timeframe are classified as non-compliant and may be quarantined. Under normal circumstances, non-compliant workstation owners and/or their respective administrative departments will be provided a warning seven days prior to removal from the network and/or quarantining.

If there is an active exploit with a potential Critical or High severity (impact) combined with a Very High or High likelihood, the removal from the campus network and/or quarantine may be immediate until successfully patched as determined by the Information Security Office.

4.11 Exceptions

Lab computers that are available for use are exempted from patches during the academic semester and when classes are in session in the summer if they are running a tool that reverts to the original image after each log in (e.g. Deepfreeze).

If an exception is requested for a workstation, application title, or specific vulnerability, an Information Security Exception Form must be submitted and approved by the Information Security Office.

- All appropriate vulnerabilities must be listed.
- Justification and mitigation steps must be provided.
- Exceptions must be signed by the appropriate Vice President.

The Information Security Exception Form is available at https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-vulnerabilityexceptionrequestform.pdf

Long term exceptions will be periodically evaluated and reviewed on an ongoing basis to determine risk exposure and applicability to university assets.

4.12 Internal Secure Network

The internal secure network is intended for use by legacy equipment and academic development. A request can be submitted to add a workstation that does not meet the vulnerability management or

workstation supplemental standards. Access to workstations in the internal secure network is limited to campus or potentially VPN access only.

4.13 Anti-virus Software

The campus supported anti-virus software must be installed, running, and updates on all campus owned workstations. For the currently supported solution, see the Common Workstations Standards at: https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-commonworkstation-standards1.pdf.

4.14 Special Consideration

If a patch is known to cause instability or other issues that can affect the campus academic or work environment, a special exemption consideration can be made. These considerations must be approved by the acting Information Security Officer. A completed Information Security Exception Form may be required after the exemption is granted.

4.15 Vulnerability Scanning Requirements

Workstations also require vulnerability scanning to meet the Enterprise Management standard in the Common Workstation Standards https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-commonworkstation-standards.pdf and the Vulnerability Management standard of the High Risk Workstation Standards https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-highriskworkstation-standards1.pdf. The current campus supported agent is Qualys VMDR.

5.0 Definitions

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

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

VLAN – The Virtual Local Area Network is a segmented section of a physical network that can have rulesets and configurations that are different than the rest of the physical network. A VLAN can be set up to be more restrictive and secure and can “wall off” traffic from the rest of the network or the internet.

Confidentiality – Keeping information secure that should not be shared. Focus is to prevent unauthorized disclosure of information.

Integrity – Keeping information and systems intact. Focus is on prevention of unauthorized modification of assets, either data or systems.

Availability – Keeping access possible. Focus is on ensuring required access to resources remains available.

Threat – Anything that can cause harm to a system.

Exploit – A means that a threat uses to take advantage of a vulnerability.

Likelihood – Probability that an event will occur.

Impact – Harm that could be caused by an event.

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
4/20/2021	Information Security Office Staff	Draft created
4/21/2021	Information Security Office Staff	Reviewed
5/5/2021	IT Collaboration Governance Group Meeting	Reviewed
5/26/2021	Information Security Office	Draft updated
5/26/2021	IT Collaboration and Standards Group Meeting	Reviewed
11/19/2021	Information Security Office	Sections 3.0 (Assigned Desktop Support Personnel), 4.3, and 4.15 updated based on IT feedback and vulnerability scanning audit finding
11/22/2021	Information Security Office	Sent for recommendation for approval
2/23/2022	ISO, AITC Representative, Director for Records & Policy	Approved for publishing