1.0 Introduction

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 web applications, server and workstation software, as well as 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

Implements: CSU Policy ISO Domain 6: Organization of Information Security Policy

Policy Reference: https://calstate.policystat.com/policy/15698973/latest/#autoid-8bxnb

Implements: CSU Policy ISO Domain 12: Operations Security Policy

Policy Reference: https://calstate.policystat.com/policy/15698973/latest/#autoid-wj683

Implements: CSU Policy ISO Domain 14: Systems Acquisition, Development and Maintenance

Policy Reference: https://calstate.policystat.com/policy/15698973/latest/#autoid-rdr9j

2.0 Scope

This standard applies to all devices and web applications connected to or hosted by the CSU Sacramento network, including but not limited to, servers, workstations, applications, web applications, network appliances, cameras, printers, and multi-function copiers.

3.0 Roles & Responsibilities

Information Security Office (ISO)

- Develop and maintain vulnerability management documentation and training.
- Maintain asset groups for business areas.

- Monitor compliance.
- Schedule weekly authenticated server vulnerability scans.
- Work with developers to schedule monthly web application scans for all production and stage web applications.
- Identity non-compliant systems and contact system owners and business area administrators prior to removal from campus network.
- Manage the removal of non-compliant systems and applications from campus network.
- Document security exceptions for non-compliant systems where risk will be accepted.

System and Web Application Owners

- Register servers and web applications in the Application Inventory system (Servicenow)
- Add servers and web applications as assets in Qualys.
- Configure servers and web applications for appropriate authenticated vulnerability scans (coordinated with ISO).
- Perform vulnerability scans and mitigate any high severity vulnerabilities prior to moving servers/application into production.
- Schedule on-going vulnerability scans.
- Review weekly vulnerability scan reports.
- Mitigate high severity vulnerabilities within the required mitigation schedule

This procedure applies to all devices and web applications connected to or hosted by the Sacramento State network, including but not limited to, servers, applications, web applications, workstations, network appliances, camera surveillance systems, printers, and multi-function copiers.

4.0 Standards

4.1 Required Vulnerability Management

Devices and information assets, including servers and web applications connected to the campus network, must be scanned in accordance with campus vulnerability management requirements. Non-compliant devices and those devices which represent a risk to the confidentiality, integrity, and availability of campus information systems are subject to removal from the campus network and quarantine.

4.2 Use of Vulnerability Scanner

While there are numerous tools that can provide insight into the vulnerabilities on a system, not all scanning tools have the same set of features, Sacramento State University's Information Security Office is responsible for approving and overseeing campus use of an enterprise scanning and assessment tool. Use of any other vulnerability scanner must be justified in writing and approved by the Information Security Officer. The scanning tool is Qualys*.

4.3 Development Lifecycle

All servers and web applications that are placed into production must be entered into the campus applications inventory.

Servers and web applications, must be scanned using authentication and web applications must be scanned using the most intrusive scan setting possible. If high-severity risk vulnerabilities are discovered, they must be remediated before the system is placed into production. A follow up scan must occur to confirm the system is cleared of high-severity risk vulnerabilities.

4.4 Scan Frequency

All campus servers will be scanned using authentication on a weekly basis.

All web applications must be scanned for vulnerabilities at a minimum of once a month, and during the development lifecycle at a time and date scheduled by the application administrator.

The application administrator should provide a clone of their application for scanning to prevent data corruption or loss of availability of the web application. Severity 4 and 5 vulnerabilities must be remediated in accordance with the remediation schedule listed in the table below.

4.5 Vulnerability Severity Scale

When scanning for vulnerabilities, findings are rated on a 1-5 severity scale, with 1 being low to no risk and 4 and 5 being critical and easily exploitable risks. The priority of all system administrators must be on the remediation of severity 4 and 5 vulnerabilities before addressing lower risk vulnerabilities.

* - For the purposes of reporting, potential vulnerabilities will be out of scope.

Severity Scale

Description

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.

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.

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.

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.

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

Potential false positives: Any vulnerability identified as a false positive must be verified using an authenticated vulnerability scan. Disputed results must be reported to the ISO and will be verified with the scanning vendor.

Confirmed false positives: these may be excluded on a per system/QID basis.

Vulnerability exceptions, especially vulnerabilities located on lower risk systems with adequate compensating controls are to be expected. In some cases these vulnerabilities are the result of hardware or software vendor responsibilities. In this case, documentation and communication of risk may be adequate.

4.6 Vulnerability Mitigation and Patching Schedule

Patchable Severity 3, 4 or 5 Vulnerabilities must be addressed within 30 calendar days from detection. Zero-day vulnerabilities may be exempt from blackout and brown-out freeze periods.

4.7 Enforcement

Servers and web applications not remediated within the required remediation schedule or timeframe are classified as non-compliant and will be quarantined.

Under normal circumstances, non-compliant server and web application owners and their respective administrative departments will be provided a warning 7 days from detection prior to removal from the network and quarantined.

4.8 Exceptions

If an exception is requested, the system or application administrator must provide the Information Security Office a risk exception form with the appropriate administrator's signature.

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

Exception Justification Form (link out in final published version)

4.9 Vulnerability Management for Desktops and All Other Networked Devices

All computing devices must be registered within the common campus Microsoft System Center Configuration Manager Infrastructure (SCCM), JAMF, and campus server and application inventories. Desktops and all other networked devices may be scanned based on risk or network environmental factors.

4.10 Vendor Maintained Systems

Vendor maintained servers and web applications hosted on the University network are subject to the same standards outlined in this document. The department that purchased the vendor's product is responsible for reporting vulnerabilities to the vendor. The vendor must be made aware by department of the University's remediation schedule and remediate vulnerabilities accordingly. If the vendor is not able to follow this schedule the department must provide an exception justification, signed by an appropriate Administrator, to the Information Security Office.

Vendor maintained Servers or Web Applications hosted off campus are not in scope of this standard. **Under no circumstances should such systems be scanned using campus tools without expressed written consent by the vendor.**

4.11 Internal Secure Network

The internal secure network is intended for use by legacy equipment and academic development. Access to systems and web applications in the internal secure network is limited to campus or potentially VPN access only.

5.0 Definitions

CMDB - Change Management Database

SCCM – Microsoft System Center Configuration Manager – Common campus infrastructure used to centrally maintaining an inventory of on-campus workstations.

Confidential Data / Personal Identifiable Information – Information that can be used to identify, contact or locate an individual or to identify a person in a single context. This is defined as level 1 data both by the CSU and California State University, Chico.

Staging/Pre-Production – a website that is identical to the production website and can be used for testing and review without consequence to customers. When scanning occurs on this site it is recommended that the site is not connected in any way with production data on the back end.

Production – This is the live, customer facing environment of an application.

Risk – Risk is the likelihood of an event occurring and the impact that event would have on an information technology asset.

Server – A combination of the hardware, operating system, application software, and network connection. A server can include, and not limited to:

- Maintains a client-server architecture
- Manages files, services and other networked resources for authorized clients or applications
- Is operationally bound to applications which it hosts
- Has the ability to handle multiple connections and requests
- May utilize virtualized hardware or software

System Administrator or Application Administrator – The individual or department responsible for the overall implementation and maintenance of a computing device.

Vulnerability – A Vulnerability is a design flaw or mis-configuration which makes a server susceptible to malicious attacks from local or remote users. Vulnerability severity levels are represented on a 1 to 5 scale, with 5 representing the highest severity.

Web Application – Any device or system connected to the Sacramento State that is coded in a browser supported programming language and reliant on a common web browser to render the application executable. Third party web applications and systems that have been created by a vendor and used by the University may be in scope of this document.

Discovery Scanning - A discovery scan is non-intrusive and intended to identify servers, workstations, or web applications, which may be unaccounted for from regularly scheduled vulnerability scans. Discovery scans are limited to scanning systems and web applications residing on the campus network. These scans will be conducted every 30 days. The Information Security Office will analyze results following each scan to identify new assets.

Non-Complaint System

A system, server, or application which has exceeded established mitigation timelines defined in the Vulnerability Management Standard will be removed from the campus network or otherwise isolated 7 days from departmental notice.

Quarantine

To modify, isolate, or remove network access.

Security Exception Form

Form and process utilized to identify non-compliant systems, document mitigation efforts, and accept risk.

7.0 Documentation Review and Approval

Review/Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
8/1/2018	ISO – Mark Hendricks	Review.
11/13/2020	IRT/ISO	Review with IRT IT Infrastructure.
12/9/2020	IRT/ISO	Update draft.
2/5/2021	AITC	Presented to AITC for review/comments.
2/22/2021	IRT, AITC	Receive comments/feedback from AITC.
3/1/2021	IRT, Director of Policy and Records Management	Recommended for approval/publication.
3/8/2021	Cabinet	Approved.
3/23/2024	IRT/ISO	Updated section 4.6
7/8/2024	CISO – N. Zierfuss-Hubbard	Updated section 4.6 90 days to 30 days, section 4.9 added JAMF, new CSU policy links