Standard: Vulnerability Management and Assessment

Executive Summary

San Jose State University (SJSU) is highly diversified in the information that it collects and maintains on its community members. It is the university's responsibility to be a good steward and custodian of the information that it has been entrusted, which must be upheld by all members of the university. Per CSU Information Security Policy 8045.0 Section 500, San Jose State University (SJSU) is required to implement appropriate controls to monitor and scan network resources and information systems to identify and remediate vulnerabilities on networked computers. Proactively managing vulnerabilities can provide vital information to management and computer administrators of known and potential vulnerabilities for our organization to mitigate the vulnerabilities and improve SJSU's security risk posture. As a result, it could save the organization resources and time otherwise needed to respond to incidents after exploitation has occurred. Vulnerability Management and Assessment standard defines the requirements for vulnerability management and assessment for all SJSU computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed and transmitted by SJSU.

Information Security Standards

Vulnerability Management and Assessment

Standard #	IS-VMA	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	5.0	Contact	Information Security Team	Phone	408-924-1530

Revision History

Date	Action
5/26/2014	Draft sent to Mike
12/1/2014	Reviewed. Content suggestions. Added comments. Hien Huynh
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.
11/18/2020	Reviewed. Nikhil Mistry
10/20/2021	Reviewed & Grammar. Cole Gunter
10/3/2022	Reviewed and Updated. Cole Gunter

Table of Contents

Executive Summary 2
Introduction and Purpose 5
Scope 5
Standard 5
- Management of Technical Vulnerabilities 5
  - Patching Application 5
  - Antivirus Application 5
  - Vulnerability Advisories and Intelligence Feeds 5
  - Periodic Vulnerability Scanning of Internal Network 5
  - Vulnerability Scanning of Internet Exposed Network 5
  - Security Advisory Patch Management 6
  - On-Going Third Party Security Configuration Scanning 6
  - Vulnerability Scanner supporting CVE and SCAP 6
  - Authenticated/Unauthenticated User Vulnerability Scanning 6
- References 6

Introduction and Purpose

This standard defines the requirements for vulnerability management and assessment for all San Jose State University (SJSU) computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by SJSU.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary (“campus”) computer systems and facilities, with a target audience of SJSU Information Technology employees and partners.

Standard

Management of Technical Vulnerabilities

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. Timely information about technical vulnerabilities of information systems being used should be obtained, the campus's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Patching Application

All systems must use an approved patching application. Required patches for servers and endpoints must be installed at minimum every 30 days.

Antivirus Application

All desktops, laptops and servers must utilize an approved antivirus/antimalware application. This includes all Operating Systems including but not limited to Windows, OSX and Linux. Any exceptions must be documented and approved by the Information Security Team.

Vulnerability Advisories and Intelligence Feeds

On at least a weekly basis, systems administration staff must review all information security vulnerability advisories issued by trusted organizations for issues affecting campus systems. Administrators will subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis.

Periodic Vulnerability Scanning of Internal Network

Each campus IT department must run and approve automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.

Vulnerability Scanning of Internet Exposed Network

To ensure that SJSU technical staff has taken appropriate preventive measures, all systems directly-connected to the Internet must be subjected to an automated risk analysis performed via approved vulnerability scanning software at least once a month.

Security Advisory Patch Management
All security advisory patches for known vulnerabilities issued by a vendor must be promptly tested and installed within the time frame required by the Information Security Team.

On-Going Third Party Security Configuration Scanning
All SJSU computers accessible from the Internet, as well as all internal production computers, must be regularly scanned by a reputable third party security vulnerability scanning service.

Vulnerability Scanner supporting CVE and SCAP
The vulnerability scanner used by SJSU will support the identification of vulnerabilities based on CVE ID as well as SCAP configuration based vulnerabilities, where applicable.

Authenticated/Unauthenticated User Vulnerability Scanning
Vulnerability scanning should run in authenticated user mode, where possible, with agents running locally on each end system to analyze the security configuration or with remote vulnerability scanners that are given administrative rights on the systems tested. A dedicated account for authenticated vulnerability scans should be used, with the account limited and used only for vulnerability testing.

References
CSU Information Security Policy -8045.0 Information Security Policy-Section 500 Information Asset Monitoring.