1.0 Introduction

Servers and web applications with high-severity vulnerabilities falling beyond an approved remediation schedule are classified non-compliant and will be quarantined. The responsible department, system and/or application owner(s) will be notified 30, 60, and 90 days in advance of a system becoming non-compliant to advise of a possible quarantine if risk remediation is not followed. A department will normally be provided a 7-day warning once a system has become non-compliant that a system will be removed from the campus network and be quarantined until appropriate remediation steps can be taken.

Implements: CSU Policy ICSUAM 8045 Information Security

Policy Reference: https://calstate.policystat.com/policy/6606971/latest/

Implements: CSU Policy ICSUAM 8100 Responsible Use Policy

Policy Reference: https://calstate.policystat.com/policy/6607908/latest/

Implements: CSU Policy ICSUAM 8080 Physical Security

Policy Reference: https://calstate.policystat.com/policy/6607762/latest/

2.0 Purpose

This procedure establishes the steps to be followed when a non-compliant system, service, device, or application has been identified for removal or isolation from the general campus network.

3.0 Scope

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

4.0 Procedure

4.1 Seven Day Notification

System Owners, application owners, departments and colleges will be notified that a system or application identified as non-compliant has been scheduled for quarantine.

Departments must patch, otherwise mitigate, or request a security exemption (Vulnerability Exception Request Form – (https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-security_exception_form.pdf).

4.2 Security Exceptions

4.2.1 Vulnerability risk exceptions may be initiated through the Exception Justification procedure. (https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-vulnerabilityexceptionprocedure.pdf) .

4.2.2 Systems and applications with approved risk exceptions will not be quarantined.

4.2.3 Security exceptions must be signed by the dean, responsible administrator, and appropriate Vice President, and be renewed every 90 days following approval.

5.0 Definitions

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.

6.0 Remote Computer Security Requirements

The CSU reserves the right to temporarily or permanently suspend, block, or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of CSU resources or to protect the CSU from liability.

Vulnerability Exception Procedure - https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-vulnerabilityexceptionprocedure.pdf

7.0 Documentation Review and Approval

Review/Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
8/2/2018	IRT/ISO	Create draft.
11/13/2020	IRT/ISO	Review with IRT IT Infrastructure.
12/9/2020	IRT/ISO	Update draft.
1/20/2021	IT Collaboration and Standards Group Meeting	Draft presented to campus IT personnel in and feedback solicited.
3/1/2021	IRT, Director of Policy and Records Management	Recommended for approval/publication.
3/8/2021	Cabinet	Approved.