Vulnerability Management for Servers	Procedure No.	ITS-2019-P	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	2-15-17	Revised:	
				Page 1 of 19

Table of Contents

1 Introduction and Purpose

As cyber-crime continues to escalate globally, the University must focus on the continuous monitoring, identification and mitigation of information security vulnerabilities in its networks, servers, systems, computers and mobile devices. Failure to do so may allow attackers to penetrate our networks and systems, and steal confidential, private and proprietary information assets.

CSU Information Security Policy (Section 8020.0, Information Security Risk Management) requires that each campus develop and maintain a risk management process that identifies, assesses, monitors and remediates risks to information assets containing Levels 1 and 2 Confidential Data as defined in *ITS-2006-S Information Classification, Handling and Disposal*. Risk assessment is an ongoing and fluid process that requires periodic review and reassessment.

Information Technology Services is responsible for ensuring effective procedures and controls are in place to maintain high levels of system and application security of the servers and systems managed within the data center. Since network devices provide incoming and outgoing access points to and from servers, all such network devices are incorporated into this procedure.

Departments that manage decentralized servers are responsible for ensuring they have procedures and controls in place to meet all audit compliance requirements. Specific requirements are outlined in Section 3.3.

2 Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein.

ID/Control #	Description	Title
8020.0	**Policy**	**Information Security Risk Management**
8020.S000	Standard	Information Security Risk Management – Exception Standard
8020.S001	Standard	Information Security Risk Management – Risk Assessment Standard
8045.0	**Policy**	**Information Technology Security**
8045.S200	Standard	Malicious Software Protection
8045.S300	Standard	Network Controls Management
8045.S301	Standard	Boundary Protection and Isolation
8045.S302	Standard	Remote Access to CSU Resources
8045.S400	Standard	Mobile Device Management
8045.S600	Standard	Logging Elements
8050.0	**Policy**	**Configuration Management**
8050.S300	Standard	Configuration Management – Mobile Device Standard *(in development)*

8050.S400	Standard	Configuration Management – Common Servers Standard *(in development)*
8050.S500	Standard	Configuration Management – High-Risk Server Standard *(in development)*

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3 Responsibilities

Responsibilities are shared across the ITS division and departments that manage department or discipline-specific servers (a.k.a., decentralized systems) within their respective areas.

3.1 Director, IT Security and Compliance

The director may designate these tasks to the IT Security compliance analyst or the network security analyst, as appropriate.

- Interprets and administers the CSU Information Security Policy as it affects servers, critical servers, networks and systems.
- Determines appropriate compliance steps and develops the procedures necessary to identify and manage server and network risks.
- Manages and oversees the vulnerability scanning business process
    - Configures the vulnerability scanner.
    - Schedules the vulnerability scans
    - Analyzes and prioritizes the vulnerability reports.
- Analyzes the vulnerabilities to determine the associated risks and provides input on risk remediation.
- Chairs regularly scheduled vulnerability management meetings consisting of ITS managers, asset owners and system administrators to review vulnerabilities and define remediation efforts.
- Notifies appropriate individuals when uncommon vulnerability tests must be executed.
- Processes requests for vulnerability scans on an as-needed basis.
- Reviews vulnerability test results after the director of IT Infrastructure has reported successful remediation efforts.
- Follows up with ITS managers, asset owners and system administrators regarding non-response to remediating risks.
- Reviews exceptions at regularly scheduled vulnerability management meeting to validate that exceptions are still appropriate.
- Serves as final approver for exception requests.
- Monitors the remediation progress against the Remediation Service Level to ensure vulnerabilities are fixed in a timely manner.

3.2 Director, IT Infrastructure Services

The director may designate or share these tasks with the assistant director, IT Infrastructure Services, as appropriate.

- Reviews the weekly vulnerability reports.
  - Directs the ITS technical remediation efforts as a result of detected vulnerabilities.
- Participates in the regularly scheduled vulnerability management meetings.
- Reviews server inventory and provides information to the director, IT Security and Compliance.
- Reviews exceptions at least quarterly to validate that exceptions are still appropriate.
- Serves as secondary approver for exception requests.
- Negotiates Memorandums of Collaboration with departments for department servers housed within the data center (managed by ITS) that are connected to the campus network

3.2.1 Assistant Director, IT Infrastructure Services

- Reviews the weekly vulnerability reports.
  - Co-directs the ITS technical remediation efforts as a result of detected vulnerabilities.
- Maintains server inventory database.
- Participates in the regularly scheduled vulnerability management meetings.
- Reports changes to the server inventory to the director, IT Infrastructure Services.
- Reviews exceptions at least quarterly to validate that exceptions are still appropriate.
- Serves as secondary approver for exception requests in the absence of or delegation from the director, IT Infrastructure Services.
- Negotiates Memorandums of Collaboration with departments for department servers housed within the data center (managed by ITS) that are connected to the campus network

3.2.1.1 Server Team

As defined in approved position descriptions:

- Ensures that all servers under ITS control are properly secured.
- Ensures that server security patches and fixes are tested, validated with application administrators and installed on a timely basis.
- Reviews and implements server firewall rule modifications.
- Analyzes server error situations (Nexpose) and takes appropriate corrective action.
- Participates in the regularly scheduled vulnerability management meetings when applicable to the systems being supported.
- Monitors and evaluates the overall performance and function of the University server resources.
- Maintains metrics of server, storage and system problems and resolutions to measure effectiveness of these systems.
- Ensures that server and storage performance and utilization information is gathered and maintained.
- Assists ITCs with high-level problems

3.2.2 Manager, Network and PBX Operations

- Reviews Nexpose data weekly as provided by the IT Security team and prioritized by identified vulnerabilities for the network team.
- Participates in the regularly scheduled vulnerability management meetings when applicable to the systems being managed.

3.2.2.1 Network Team

As defined in approved position descriptions:

- Ensures that switches and routers on the network are properly secured.
- Ensures that software security patches and fixes are installed on a timely basis.
- Maintains firewall and security appliance configurations.
- Analyzes network error situations (Nexpose reports) and takes appropriate corrective action.
- Monitors and evaluates the overall performance and function of the campus network.
- Ensures that network performance and utilization information is gathered and maintained.
- Maintains metrics of network problems and resolutions to measure effectiveness of network systems.
- Performs data sanitization of all equipment prior to disposal or transfer of equipment outside of the network services group.
- Participates in the regularly scheduled vulnerability management meetings when applicable to the systems being supported.

3.2.2.2 Application Administrator

The application administrator is the individual responsible for any specific application on a decentralized system or department server. There may be multiple application administrators on a department server that supports more than one application.

- Tests the application after the security updates, patches and fixes are installed in a timely manner.
- Participates in the testing process and validates the applications work.
- Reviews Memorandums of Collaboration and provides updates on an annual basis.

3.3 Academic and Administrative Departments

Pursuant to the CSU Information Security Policy, sections 8010.0: Information Security Program and 8015.0: Organizing Information Security, all academic and administrative departments are responsible for ensuring they have procedures and controls in place for the systems they maintain. In addition, departments are responsible for minimally reporting the following to the director, IT Security and Compliance annually:

System Information

a) Server name
b) Physical location
c) ITC or individual(s) responsible for server administration
d) Email of responsible individual
e) Risk exposure mapping designation based on instructions in Section 5, Vulnerability Risk Assessment
f) Is the system connected to the campus network?
g) Is the system accessed remotely?
h) System printout of sys admin ids.

Data Information

a) Does the server house data files of multiple data owners?
b) Data owner(s) of the system data or each data file, if a multi-purpose server.
c) Email of responsible individual
d) Does the server contain Levels 1 and 2 Confidential Data?
e) If yes, is the data encrypted on the server?
f) If yes, where is the system backup data stored?
g) If yes, is the backup data encrypted?
h) System printout of user ids for systems with Levels 1 and 2 Confidential Data.

3.3.1 Information Technology Consultants (ITCs) or Asset Owners

- Ensures that all decentralized managed server(s) under their control are properly secured.
- Ensures that server security patches and fixes are tested and installed on a timely basis.
- Reviews vulnerability reports for their server(s) and takes appropriate corrective action.
- Accepts risks and requests an exception to remediation actions.
- Monitors and evaluates the overall performance and function of their server resources.
- Participates in the vulnerability management meetings when applicable to the system(s) they manage.

4 Inventory Management

Information Technology Services is responsible for maintaining an up-to-date inventory of servers and network components under its management. This document may be required for submission to or onsite review by Board of Trustee auditors during scheduled information security audits.

Inventory changes and corrections for Property Management inventory should be initiated on any ongoing basis as changes or errors are identified.

4.1 Server Inventory

All servers purchased by the University must be tracked via the University inventory management system. A single database (MS Excel or Access) of ITS-managed servers shall be created and maintained by the assistant director, IT Infrastructure Services or designee. In consultation with the application administrator, the director of IT Security and Compliance or designee will identify the existence of Levels 1 and 2 Confidential Data and the risk exposure mapping designation.

4.2 Network Inventory

CSU Information Security Standard 8045.S300 details the minimum requirements for documenting the network structure and configuration. For the purpose of this procedure, a vulnerability risk assessment must be routinely performed on the following network devices:

a) Switches
b) Routers
c) Firewalls
d) VPN
e) Wireless Controllers
f) DNS/DHCP Appliance Servers
g) Packet shaper
h) Load balancer

5 Information Security Risk Management

Risk management involves a series of steps as outlined in CSU Information Security Policy, Section 8020.0, “Information Security Risk Management.” The general categories are detailed in the sections below and include:

- Risk assessment
- Risk monitoring
- Risk mitigation
- Risk acceptance or transference (or request an exception)

5.1 Vulnerability Risk Assessment

The first step is to develop a process for assessing risks to the University's information assets. These assessments must be based on established **severity** and **likelihood** criteria, and managed through ongoing evaluation and review activities. Every server must undergo an individual assessment and the results of the risk assessment mapping (section 5.3) must be identified in the server inventory database.

There are four steps involved in assessing vulnerability risk:

1. Determining the severity of a potential incident.
2. Determining the likelihood of an incident occurring.
3. Mapping the vulnerability risk.
4. Remediating the vulnerability in a timely manner reflective of the risk.

Note: The following scales were derived from the SANS Institute criteria by the CSU Information Security Office and the working teams comprised of campus information security officers (ISOs).

5.1.1 Severity Scale

Severity	Description
Critical	May allow full access to or control of the application, system, or communication, including all data and functionality. • Attacker is not limited in access after execution and they may be able to escalate privileges. • Possible disclosure of 500 or more records containing Levels 1 and 2 Confidential Data. • Allows modification or destruction of all critical/sensitive data. • Total shutdown of a critical service(s).
High	May allow limited access to or control of the application, system, or communication, including only certain data and functionality. • Attacker can access the sensitive data or functionality of a user. • An outside attacker can execute arbitrary code at the level of the user. • Ability for a user to access unauthorized functionality. • Allows limited modification or destruction of critical/sensitive data. • Severe degradation of a critical service(s). • Exposure of sensitive system or application information that provides implementation details that may be used to craft an exploit. • Breach may be difficult to detect.
Moderate	May indirectly contribute to unauthorized activity or just have no known attack vector. Impact may vary as other vulnerabilities or attack vectors are identified. • Weaknesses that can be combined with other vulnerabilities to have a higher impact. • Disclosure of information that could aid an attacker. • Any vulnerability that can hinder the detection or investigation of higher impact exploit, • Fines greater or equal to $10,000 and less than $50,000.

Low	May indirectly contribute to unauthorized activity or just have no known attack vector. Impact may vary as other vulnerabilities or attack vectors are identified. • Deviation from a recommended practice or emerging standard. • May be the lack of a security process or procedure to govern or manage security-related activities. • No direct exposure of data. • Fines less than $10,000. • Would not contribute to the exposure of confidential information. • Would not enable alternation of stored records. • Would not impact the availability of critical University systems.

5.1.2 Likelihood Scale

Severity	Description
Very High	Exposure is apparent through casual use of publicly available information, and the weakness is accessible publicly on the internet. • Can be exploited by large anonymous population (Any internet host). • Vulnerability can be exploited from the general internet. • Possible with only publicly available information. • No specific attack skills are required, such as general user knowledge.
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. • Can be exploited by extended campus population (students, guests). • Can be exploited by anyone that can reach the network with no authentication required. • Vulnerability can only be exploited from related networks to which the University does not control access (vendors). • Simple (easily guessable) authentication may be required for exploit. • Possible with limited knowledge or target configuration. • Basic attack skills are needed, such as an automated attack (i.e., there exists a metasploit module, or known attack).
Moderate	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. • Can be exploited by a limited and know population. • Vulnerability can be exploited through the internal University network or client connection only. • Simple authentication is required for exploit. • Vulnerability requires a user to be “tricked” into taking some action (e.g., a targeted phishing message or a request to go to a website and download a file). • Possible only with detailed internal information or reasonable guessing. • Expert technical knowledge is needed, such as knowledge of available attacks tools

Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede the vulnerability from being exercised. • Threat source is an employee. • Vulnerability can be exploited through the internal University network only. • Single strong authentication is required for exploit. • Possible only with a significant amount of guesswork or internal information. • Vulnerability can be exploited with local physical access only and resources have physical access controls, but are still accessible to a large number of people.
Negligible	The threat source is part of a small and trusted group or controls prevent exploitation without physical access to the target or significant inside knowledge is necessary, or purely theoretical. • Small and trusted population. • Vulnerability can be exploited with local physical access only and resources have strong physical access. • A series if strong authentications or multi-factor authentication are required for exploit. • Possible only with a significant amount of likely detectable guesswork or tightly controlled internal information. • Attack is theoretical in nature and no known exploit or potential of exploit is currently proven or expected.

5.1.3 Risk Exposure Mapping

Based on the results identified for each individual server in Section 5.1, Severity Scale and Section 5.2, Likelihood Scale, the overall risk exposure can be identified from the following table.

		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

5.1.4 Remediation Timetables

Severity	Remediation Service Level
Critical	20 days
High	45 days
Moderate	90 days
Low	180 days

5.2 Vulnerability Scan Targets

All servers connected to both public and private network segments must be scanned on a consistent schedule.

5.2.1 Scanning Tools

The table below specifies the approved scanning tools.

ID/Control Number/ Model #	Description
Nexpose	Provided through Rapid7, the vulnerability management program provides data in real time with granular risk scores.

5.3 Vulnerability Scan Frequency

In addition to regularly scheduled scans, by-request or as-needed requests may be issued by the director, IT Security and Compliance when circumstances are warranted (e.g., identified, reported or suspected intrusion; audit request for documentation).

- Systems are scanned weekly using a rolling scan.
- Scans are scheduled sequentially to ensure the least amount of impact to the infrastructure.

5.4 Vulnerability Reporting

The following Nexpose vulnerability reports are available:

- Baseline Comparison – Compares current scan results against an earlier scan.
- Executive Overview – High level overview of systems with statistical overview.
- Highest Risk Vulnerabilities - Provides information and metrics about 10 discovered vulnerabilities with the highest risk scores.
- PCI Reporting: PCI Attestation of Scan Compliance, PCI Executive Summary, PCI Host Details or PCI Vulnerability Details.
- Remediation Plan: Provides detailed remediation instructions for each discovered vulnerability.
- Report Card: Lists test results for each discovered vulnerability, including how it was verified.

- Risk Scorecard: Grades sets of assets based on risk, and provides data and statistics for determining risk factors.
- SANS Top 20
- Top 10 Assets by Vulnerabilities: Lists total vulnerabilities, and malware and exploit exposures for 10 assets with the most vulnerabilities.
- Top 10 Assets by Vulnerability Risk: Lists risk scores, total vulnerabilities, and malware and exploit exposures for 10 assets with the highest risk scores.
- Top Policy Remediations: Lists top policy compliance remediations as prioritized by policies that ITS selects.
- Top Policy Remediations with Details: Lists top policy compliance remediations as prioritized by policies that ITS selects. Also provides steps for each remediation and lists each affected asset.
- Top Remediations: Lists top remediations as prioritized by vulnerability-related criteria that ITS selects.
- Top Remediations with Details: Lists top remediations as prioritized by vulnerability-related criteria that ITS selects. Also provides steps for each remediation and lists each affected asset.
- Vulnerability Trends: Tracks trends for vulnerabilities found, assets scanned, malware kit and exploit exposures, severity levels, and vulnerability age over a date range that you select.

The following options are provided to system owners for vulnerability report preferences:

- File format: PDF, RTF, XML, HTML or text
- Asset(s) or asset group(s)
- Frequency: Recurring on a schedule, recurring after every scan (based on start date and time and repeating every number of hours, days, weeks, months)
- Include risk trends over a date range (1 year, 6 months, 3 months, past month or custom range)
- Define report on a baseline scan
- Distribution: email a URL, file or zip file

Based on the system owner's report of choice, schedule and delivery method, vulnerability reports will be generated based on the information identified in the inventory database and will be delivered to system owners, system administrators and management as proof that a scan has occurred.

Systems are organized into groups so that devices and vulnerabilities can more easily be distributed to staff. A device may belong to one or more groups. Groups can be added or changed by any of the system administrators with the approval of the director, IT Security and Compliance. Below is a listing of key reports that are automatically generated and delivered.

Status Report	Frequency	Purpose
Executive Overview of Critical Asset Group – Trending over 3 Months	Weekly	Provided to management for review to identify vulnerability status changes and trends on asset groups identified as critical risk.
Executive Overview of High Asset Group – Trending Over 3 Months	Weekly	Provided to management for review to identify vulnerability status changes and trends on asset groups identified as high risk.
Top 10 Vulnerable Servers Report to ESG (Critical Asset Group)	Weekly	Provided to the server team and management for review to identify those top 10 critical identified servers that have the top 10 risk score based on vulnerabilities
Top 10 Vulnerable Servers Report to ESG (External Facing Asset Group) – Monthly Scan	Monthly	Provided to the server team and management for review to identify those top 10 external accessible servers that have the top 10 risk score based on vulnerabilities

5.5 Remediation Management

Vulnerability reports provide ITS and department server data owners and administrators with the tools to identify and evaluate the potential risk to University information assets that may be exposed by system vulnerabilities. Proactive steps can then be taken to address the identified vulnerabilities.

Remediation management is a shared responsibility encompassing IT Security and Compliance, IT Infrastructure, System Administration, Network Operations, and departments and their ITCs as required. Dissemination of actionable weekly system reports and prioritization discussions are conducted at regularly scheduled vulnerability management meetings. Unplanned reports and alerts that are determined to be critical are remediated within the guidelines of Section 5.4.

The tables below outlines the general remediation responsibilities by role.

5.5.1 Information Technology Services

IT Security Team	
The IT Security team maintains the scanning and reporting from the vulnerability management tool (Nexpose), generates reports, and monitors the vulnerability situation of the University for audit compliance. The security team ensures that systems are scanned for vulnerabilities on a regularly scheduled basis and that identified vulnerabilities are brought to the attention of the appropriate personnel.	• Monitor Nexpose weekly for vulnerabilities in critical risk systems. • Monitor Nexpose weekly for vulnerabilities in high risk systems. • Analyze the vulnerability reports and determine the associated risks. • Distribute vulnerability reports. • Manage the reports and vulnerability database. • Track the vulnerability remediation progress. • Report unmitigated vulnerabilities of significance to executives. • Respond to requests for vulnerability reviews from other departments. • Review and approve exception requests. • Maintain a database of servers and systems containing sensitive data for audit compliance.
IT Infrastructure System Owner for all Data Center and ITS-managed Department Servers	
System owners work with the system administrators to authorize, prioritize and schedule changes to their systems, or implement acceptable mitigating controls to reduce the risk to an acceptable level. Corrective actions, such as patches, are considered normal business maintenance. However, if other mitigating controls are used, teams should review and approve the controls as appropriate to address the vulnerability. It is ultimately the system owner's responsibility to accept any unmitigated risk that remains.	• Review vulnerability reports. • Assess the degree of risk that the vulnerabilities represent. • Review and approve proposed corrective actions or mitigating controls. • Schedule changes with the users and the system administrators. • Formally (in writing) accept unmitigated risks and explain mitigating controls. • Submit exception requests when required.

System Administrators	
System administrators implement the corrective actions authorized by the system owners. They are technical resources that may research and propose various resolutions and mitigating controls.	• Review vulnerability reports. • Review the risk of vulnerabilities from a technical perspective and determine if patches are available or if a configuration change is required. • Propose corrective actions or mitigating controls to the managed system. • Request vulnerability exceptions where appropriate. • Implement changes authorized by the system owner(s)

5.5.2 Department Servers

Department servers are often located within the department or division and the system administrator is generally the assigned ITC or a faculty owner. Some department servers are located in the ITS data center but are managed by the department, not ITS. Those data center servers are included herein. Department servers managed by ITS are included in Section 9.1.

IT Security Team	
The IT Security team maintains the scanning and reporting from the vulnerability management tool (Nexpose), generates reports, and monitors the vulnerability situation of the University for audit compliance. The security team ensures that systems are scanned for vulnerabilities on a regularly scheduled basis and that identified vulnerabilities are brought to the attention of the appropriate personnel.	• Monitor Nexpose weekly for vulnerabilities in critical risk systems. • Monitor Nexpose weekly for vulnerabilities in high risk systems. • Distribute vulnerability reports. • Manage the reports and vulnerability database. • Track the vulnerability remediation progress. • Report unmitigated vulnerabilities of significance to executives. • Respond to requests for vulnerability reviews from other departments. • Review and approve exception requests. • Maintain a database of servers and systems containing sensitive data for audit compliance. • Propose corrective actions or mitigating controls to the asset owner(s) or ITC(s).

Department Decentralized System Owner	
System owners work with the system administrators to authorize, prioritize and schedule changes to their systems, or implement acceptable mitigating controls to reduce the risk to an acceptable level. Corrective actions, such as patches, are considered normal business maintenance. However, if other mitigating controls are used, teams should review and approve the controls as appropriate to address the vulnerability. It is ultimately the system owner's responsibility to accept any unmitigated risk that remains.	• Review vulnerability reports. • Assess the degree of risk that the vulnerabilities represent. • Review and approve proposed corrective actions or mitigating controls. • Schedule changes with the users and the system administrators. • Formally (in writing) accept unmitigated risks and explain mitigating controls. • Submit exception requests when required.
Information Technology Consultants	
ITCs implement the corrective actions requested by the IT Security Team. They are technical resources that may research and propose various resolutions and mitigating controls.	• Review vulnerability reports. • Assess the risk of vulnerabilities to the system. • Propose corrective actions or mitigating controls to the system owner(s). • Request vulnerability exceptions where appropriate. • Implement changes authorized by the system owner(s)

5.6 Exceptions Management

Vulnerabilities may exist that cannot be remediated for several reasons. For example, some vendor appliances may not be patchable, along with services that may be exposed for proper application operation, or end-of-life systems may remain in operation but are no longer supported by the vendor. Exceptions must be requested through IT Security and Compliance and must include reasons for the exceptions.

5.6.1 Exception Request Types

Reasons for exceptions can fall under any of the following categories:

1. Compensating Controls – There is a means for mitigating the risks around the vulnerability.
2. Acceptable Use – Some use for applications might be interpreted as a vulnerability but its use may be acceptable under certain practices.
3. Acceptable Risk – Some situations pose low risk, but actions to remediate are too costly or an applications will fail if the vulnerability is remediated.

4. False Positives – If a report shows a vulnerability is a false positive, there must be some form of documentation to show that the report has been tested and verified. The exception report for a false positive must include names of individuals involved in testing, requesting and approving the exception, relevant dates and information about the testing.

5.6.2 Submitting Exception Requests

To allow for these conditions, exception requests can be submitted in writing to the director, IT Security and Compliance by any IT Infrastructure director or manager responsible for servers or network devices. Exception requests are never permanent and must be reviewed periodically by the IT Security and Compliance office to prevent an approved exception being permanently ignored. All exception requests must include the following:

- The exception type *(See Section 5.6.1)*
- Justification for the request
- The expiration date

If the vulnerability has the following exception status…	***…and the following permission exists…***	***…take the following action:***
Never been submitted for an exception	Submit exception request	Submit an exception request
Previously approved and later deleted or expired	Submit exception request	Submit an exception request
Under review (submitted, but not approved or rejected)	Review vulnerability exceptions	Approve or reject the request
Excluded for another instance, asset or site	Submit exception request	Submit an exception request
Under review (and submitted by you)		Recall the exception
Under review (submitted, but not approved or rejected)	Delete vulnerability exceptions	Delete the request
Approved	Review vulnerability exceptions	View and change the details of the approval, but not overturn the approval
Rejected	Submit exception request	Submit another exception request
Approved or rejected	Delete vulnerability exceptions	Delete the exception, thus overturning the approval

5.6.3 Reviewing Exception Requests

Exception requests are reviewed by the vulnerability management team at each regularly scheduled meeting. New requests will be recorded on the vulnerability management tool with a notation of "under review" in the Review Status column. Following review, the vulnerability management team will either approve or reject the request. Approved requests can be set with an expiration date for those instances when an exception will be in effect for only a limited time. Departments will be notified of rejected requests along with an explanation of the rejection decision.

Vulnerability exceptions will continue to appear only on reports labeled Report Card under the vulnerability listing with the reason for exception.

6 Quality Assurance Provisions

6.1 Customer Relations Management

IT Security and Compliance will utilize regularly scheduled vulnerability management meetings to invite, as appropriate, ITCs, data owners and system owners from departments with decentralized systems to learn about and participate in risk assessment and vulnerability remediation practices.

6.2 Configuration Management

IT Security and Compliance is responsible for creating and maintaining a comprehensive University database of all systems and servers that contain Levels 1 and 2 Confidential Data. IT Infrastructure is responsible for updating the data center server inventory. Departments are responsible for updating their distributed system inventories.

6.3 Change Management

The IT network security analyst will issue notices to IT Infrastructure or department ITCs as vulnerabilities are identified. Discussion regarding the status of vulnerability patching will take place during regularly scheduled meetings of the vulnerability management team consisting of ITS managers, asset owners and system administrators.

6.4 Disaster Recovery/Business Continuity Management

The ITS server housing Nexpose is considered a Priority 3 restoration during a disaster recovery event. ITS will accept all risks that may be present during the recovery process so the recovery team can focus on restoring vital University services. A vulnerability assessment on all critical ITS and department servers will be conducted immediately after all services are restored. Based on the deployment of ITS staff, vulnerability assessments may or may not be continued during a business continuity event.

6.5 Security Management

IT Security and Compliance is responsible for determining that all University systems and servers containing Levels 1 and 2 Confidential Data are evaluated for vulnerabilities on a regularly schedule basis, to be determined by the criticality of the systems' data elements.

6.6 Accounting Management

IT Security and Compliance, with support and assistance from IT Infrastructure, is responsible for accountability of risk assessment schedules and remediation timeframes for audit compliance. Compilation of requested audit deliverables must be completed within 15 days of the formal CSU Board of Trustees request for documents in order for the information security officer and internal auditor to review and accept the submission as acceptable and compliant.

6.7 Fault Management

Not applicable to this procedure. By virtue of following this procedure, faults through vulnerabilities will be avoided.

6.8 Efficiency/Effectiveness Management

Efficiency and effectiveness will be measured by the following:

- Consistent on-time remediation of identified vulnerabilities as outlined in the remediation timetable, Section 5.1.4.
- Non-recurrence of remediated vulnerabilities on critical servers.
- Fewer vulnerabilities overall reported by Nexpose over time.
- Proactive server management to lessen or prevent vulnerabilities.
- 100% participation and cooperation from departments with decentralized servers.