Procedures for Vulnerability Remediation and Risk Acceptance

1. Purpose

The purpose of this Procedure is to define standards, procedures, guidelines, and restrictions for the remediation and acceptance of risk for a vulnerability discovered on a network device. This Procedure is intended to strictly outline the process and timelines for vulnerability remediation and risk acceptance and what services, and under what circumstances, risk would be accepted.

2. Scope

Weekly scheduled vulnerability scans will be conducted on devices connected to the Los Rios Community College (LRCCD) network to identify weaknesses that may allow the devices to be compromised. Those weaknesses can be in the design of the device (loophole in the device's configuration) or the way LRCCD personnel configured the device.

This Procedure applies to all LRCCD managed devices including but not limited to network electronics (switches, routers, and appliances), servers, desktops, storage area networks, and printers. Anything connected to a LRCCD network is included in this scope.

3. Definitions

Acceptance of risk is to say LRCCD is willing to accept the liability of continuing to operate with a known vulnerability that could compromise the integrity of the LRCCD network and/or damage the reputation of LRCCD.

Compromised is defined as any computing resource whose confidentiality, integrity or availability has been adversely impacted by an untrusted source.

Vulnerability Scans:

- ***External scans*** provide a comprehensive view of network vulnerabilities that could be exploited by an external entity. External scans are focused on misconfigurations in perimeter devices and public facing web servers that could allow an attacker to penetrate the network, deface or deny access to systems.
- ***Internal scans*** are scanned from a point on the system's network segment (i.e., inside the firewall) to identify vulnerabilities that could be exploited by a knowledgeable insider or an entity that has penetrated the perimeter defense.
- ***Mitigation scans*** are conducted after the identified vulnerabilities have been corrected. Mitigation scans may be conducted as a separate action or may be included in the next routine scan, depending on the sensitivity of the system and the criticality of the vulnerability.

4. Remediation Timeframes

Overview

Los Rios will leverage the Vulnerability Priority Rating system developed by Tenable to prioritize the

remediation of discovered vulnerabilities. The VPR methodology utilizes the CVSS v3 score, as well as other data points to determine the severity of the vulnerability. Using the VPR will allow us to significantly reduce the number of vulnerabilities that need to be addressed (a potential reduction of 70% or more versus strict CVSS v3 Critical/High Risk prioritization) while reducing an equivalent amount of risk.

The Tenable VPR scale is as follows:

VPR Category	VPR Range
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

Prioritization Process and Timelines:

Discovered Vulnerabilities should be addressed/remediated using the following prioritization method:

Critical VPR – Remediate within 14 days

High VPR – Remediate within 30 days

Critical Severity, No VPR score – Remediate within 30 days

High Severity, No VPR score – Remediate within 60 days

5. Appropriate Use

It is the responsibility of all system administrators to keep their systems up to date and follow best practices in configuring services. This applies to both regularly applying patches to operating systems and applications and ensuring they are running software that are actively supported.

Example of Non-Allowable Risk Acceptance Request:

- Devices not actively patched and/or supported
- Services not configured properly
- Remediation solution available

Example of Allowable Risk Acceptance Request:

- Service vendor does not agree with scanning results (official documentation/justification from

the vendor is needed for evidence)
- Risk needs to be accepted due to **critical** business needs
- Remediating extension are needed due to **critical** business operations
- Other compensation controls implemented that greatly reduce risks

6. Approval

To request the approval of a vulnerability risk acceptance, complete the Vulnerability Risk Acceptance Request Form. Ensure all information is provided to describe the vulnerability, the risks the vulnerability presents, the business justification for accepting the risk, and any applicable supporting documentation. For risk to be accepted all approval signatures must be present. Risks accepted will need to be re-evaluated bi-annually for continued approval.