Risk-Based Vulnerability Management Strategy

Department: Campus Technology	**Date Created:** 3/24/2025
Owner: IT Department	**Date Last Revised:** 4/2/2025

Printed copies of this document are for reference only.

1. Strategy Statement

The purpose of the Risk-Based Vulnerability Management Strategy is to establish standards and governance for the IT department on reporting and mitigating vulnerabilities within our infrastructure. This is to ensure vulnerabilities are classified and mitigated based on their risk to the college and are handled within their classifications.

1.1 Scope

The scope of this strategic plan applies to all IT department employees and all college-owned technology.

1.2 Exceptions

IT leadership may exclude an asset from the Vulnerability Management Strategy by completing a signed statement. This statement will acknowledge and accept the risk associated with the vulnerable system.

1.3 Vulnerability Management Strategy

The Vulnerability Management Strategy is split into several processes:

- Vulnerability Classification
- Vulnerability Tracking
- Progress Reporting

Each individual section will outline how a vulnerability is classified, prioritized, remediated, and reported to IT leadership on its status.

1.3.1 Vulnerability Classification

Vulnerabilities are classified based on their severity. Criteria are then applied according to how the vulnerabilities are discovered by the department and the extent of the risk they pose.

1.3.1.a Common Vulnerabilities and Exposures

Common Vulnerabilities & Exposures, also known as a CVE, is a standardized way to classify publicly known security vulnerabilities in technological systems, such as software, which is maintained by the MITRE corporation. Each CVE is rated with a severity level, in a scale from 1 (lowest) -10 (highest) based on the Common Vulnerability Scoring System.

The college's information technology asset management (ITAM) system tracks what CVEs are affecting college IT assets. After a vulnerability is detected and there is a known fix, the following is the IT department's timeline to remediate it:

- Critical Vulnerabilities
    - Severity score: CVSS 9 - 10
    - Remediate vulnerability within 15 business days
- High Vulnerabilities
    - Severity score: CVSS 7 – 8.9
    - Remediate vulnerability within 30 business days
- Medium or Below Vulnerabilities
    - Severity score: CVSS 0 – 6.9
    - Remediate based on staff availability

Additionally, to measure the surface area and time to remediate of a vulnerability, additional thresholds have been added to the CVS score

- If a vulnerability affects over 50% of assets
    - +0.5 to the CVSS
    - Add five additional business days for remediation
- If a vulnerability affects over 75% of assets
    - Add an additional +0.5 to the CVSS
    - Add an additional ten business days for remediation (+15 total)

All vulnerabilities must be added to the register and a remediation plan must be started within 5 business days of detection or notification to the IT department.

1.3.1.b Internally Reported Vulnerabilities

Not all vulnerabilities are classified as CVEs; they can also be identified through research, discovery, or audits. The IT department will assess the severity of all reported vulnerabilities based on the likelihood of exploitation and the potential impact that would result from exploitation.

Each factor is rated on a scale of 1 (lowest) to 5 (highest). Both factors are multiplied together and then divided by 2.5 to rate the severity of the vulnerability out of 10 to match the CVSS scale. Then the same thresholds for remediation are applied from section 1.3.1.a and the vulnerability is recorded and a plan is made for remediation.

1.3.1.c Third-Party Assessments & Risks

All third-party service providers and risks are assessed by IT leadership pursuant to the Technology Purchasing Policy. Information Security Personnel may be queried to provide analysis of any risks.

1.3.3 Tracking Risks & Vulnerabilities

Once a vulnerability is documented, information of remediation instructions will be provided to applicable IT personnel for remediation. Below is the minimum required information IT personnel must be provided to effectively remediate the vulnerability:

- A description of the vulnerability
- A list of affected assets assigned to the personnel
- The deadline for remediation
- Remediation steps

Once the assigned employee completes their remediation of their list of affected systems, they will inform the information security personnel, so the vulnerability can be marked as resolved.

1.3.4 Reporting

IT leadership will receive a monthly report of all active and remediated vulnerabilities for the previous calendar month. The report includes any late, delayed, resolved, and active vulnerabilities that are documented by the IT department, and all associated information with each vulnerability.

1.4 Enforcement

Any vulnerability in the risk register that surpasses it's deadline will be reported to the IT leadership in the monthly vulnerability report. Any issues to follow the vulnerability management strategy will also be reported by information security personnel in the report.

1.5 Strategic Plan Review

This strategic plan shall be reviewed and updated periodically by the IT department to ensure its effectiveness and compliance with relevant laws, regulations, and industry standards.

1.6 Revision history

Below is the recorded history of the plan. This must be updated each time the strategic plan undergoes changes.

Date	Change Description	Author - Position	Approved By - Position
3-24-2025	Plan creation	McLaughlin – Information Security Analyst	-
3-26-2025	Revised and reviewed the plan. Sent the plan to IT leadership for review	McLaughlin – Information Security Analyst	-
4-1-2025	Completed proposed edited requested by the CDTO. Remove watermark.	McLaughlin – Information Security Analyst, edit by Ron Wall, CDTO	-

4-2-2025	CDTO accepted changes. Prepared for approval	McLaughlin – Information Security Analyst	Ron Wall

-----END OF DOCUMENT-----