SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **VULNERABILITY MANAGEMENT**	Procedure 8.22.01

I. PROCEDURE STATEMENT

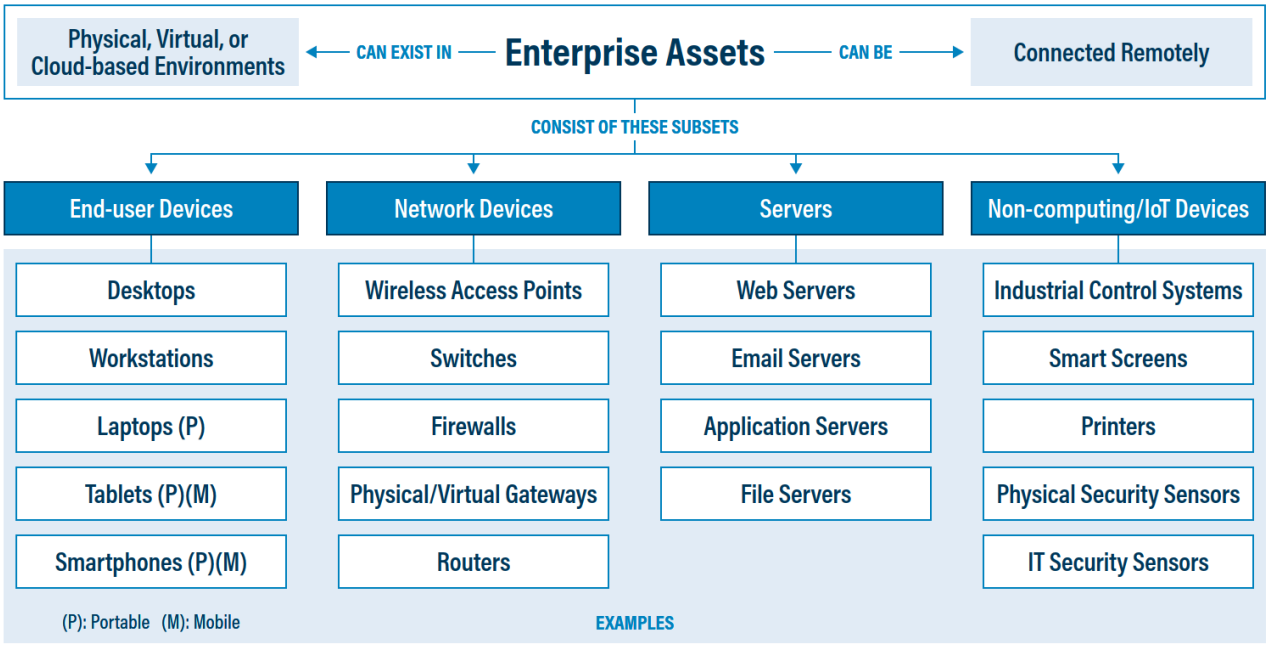
Vulnerability management is the process of searching for, prioritizing, and remediating vulnerabilities in enterprise systems and software. The *Vulnerability Management Procedure* provides the processes and procedures for ensuring enterprise assets do not contain vulnerabilities. This policy applies to all divisions and all assets connected to the College's enterprise network.

II. RESPONSIBILITY

The IT Division ("IT") is responsible for all vulnerability management functions. Specifically, administrators are responsible for assessment and application of patching. Necessary vulnerability information must be relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as required or needed. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them, such as applying updates in a regular manner or restarting their systems.

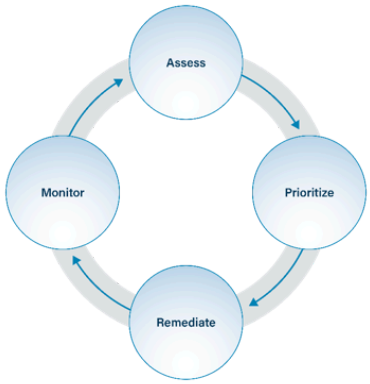
III. TYPES OF VULNERABILITIES IN ASSETS

There are many types of enterprise assets that may contain vulnerabilities. The CIS Controls define an asset as all end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments. Essentially any device owned, or system used by, an organization. Vulnerabilities may exist in all of these assets. All enterprise assets will contain vulnerabilities at some point in their lifecycle.



SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **VULNERABILITY MANAGEMENT**	Procedure 8.22.01

IV. SECURE CONFIGURATION MANAGEMENT PROCESS



Assess – A combination of automated scanning, manual analysis, and leveraging threat intelligence to ascertain if vulnerabilities exist in enterprise systems and software.

Prioritize – Creating a prioritized list of vulnerabilities that should be remediated in a specific order. This may simply be identifying and fixing critical vulnerabilities first, or using a scoring system such as the Common Vulnerability Scoring System (CVSS).

Remediate – Fixing or patching vulnerabilities to ensure they are removed or mitigated in some other way.

Monitor – Ensuring that remediated vulnerabilities are no longer affecting systems or did not introduce more problems that must be solved.

V. ASSESS

A. A process for performing vulnerability management must be established.
    1. This process must be documented and approved.
    2. At a minimum, the vulnerability management process must be reviewed on an annual basis or following significant changes within the enterprise.
    3. IT must monitor vulnerability announcements and emerging threats applicable to enterprise asset inventory.
    4. All systems connected to the enterprise network must be scanned for vulnerabilities.

VI. PRIORITIZE

A. Identified vulnerabilities must be prioritized, with more critical vulnerabilities addressed first.

VII. REMEDIATE

A. A process for remediating identified vulnerabilities must be established.
    1. This process must be documented and approved.

2. At a minimum, this process must be reviewed on an annual basis or following significant changes within the enterprise.
3. Vulnerabilities that cannot be remediated must be submitted through the vulnerability exception process.

B. Operating systems must be configured to automatically update, unless an alternative approved patching process is used.
C. Applications must be configured to automatically update, unless an alternative approved patching process is used.
D. All users of enterprise assets have a duty to install updates for business systems and applications in a timely manner.
E. All users must ensure required reboots occur within a reasonable timeframe to ensure updates are properly installed.
F. High severity vulnerabilities must be addressed as a matter of priority.

VIII. MONITOR

A. IT should subscribe to a threat information service to receive notifications of recently released patches and other software updates.
B. IT must notify the decision-making authority if vulnerabilities are not mitigated in a timely manner.
C. Every month, IT must create a report containing the status of all known vulnerabilities within the enterprise.

LEGAL REFERENCES:

- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, 7.1 (Establish and Maintain a Vulnerability Management Process) and 7.2 (Establish and Maintain a Remediation Process)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

Adopted: September 2025

Revised: N/A