CONE HEALTH	**Guideline:** ITS Vulnerability Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
System administrators

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), sensitive, and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define how the organization will proactively prevent or detect and mitigate technical security vulnerabilities.

Scope and Goals:
This procedure defines technical security assessments to be performed by the organization. The goals of this procedure are as follows.

- Define program roles and responsibilities.
- Define different types of assessments and their recurring schedule.
- Define vulnerability mitigation requirements.

Responsibilities:
Chief Information Security Officer (CISO):
The CISO is responsible for, but not limited to, the following activities:

- Revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Developing vulnerability assessment standards for the following:
    - Threat management
    - Compliance
    - System development/acquisition lifecycle (i.e., pre-production, post-production, continuous monitoring)
    - Risk management
- Selection and approval for purchase of vulnerability assessment technology solutions.
- Reviewing the technical vulnerability management program on a quarterly basis and determining if the solutions being used are still relevant and effective in identifying risk.
- Ensuring the use of reputable vulnerability scanning tools and/or services that are able to detect the latest and highest risk vulnerabilities, and that the entire covered environment is being monitored for these vulnerabilities (breadth and depth coverage).
- Reviewing all assessment results and determining mitigation strategy in accordance with risk management principles as outlined in the Information Security Risk Management procedure.
- Periodically reporting assessment results and remediation activity to senior management.

- If significant environment change takes place, ensure the relevant vulnerability test is being performed on demand.
- Subscribe to and maintain a list of credible services that monitors for new vulnerabilities related to software, technology and information resources.

Information and Technology Services (ITS):

ITS is responsible for, but not limited to, the following activities:

- Selection and implementation of vulnerability assessment technology solutions. All solutions selected will include the capability to readily update the systems they can scan and the vulnerabilities they scan for.
- Ensure that all vulnerability scanning tools are set to receive definition updates at least once daily.
- Ensure that only properly authorized and trained personnel are performing the security assessments required by this procedure.
- Restrict physical and logical access to assessment technology solutions.
- Subscribe to a credible service that monitors for new vulnerabilities pertaining to network devices and systems supported by ITS.
- Reviewing vulnerability assessment results (i.e., scans) to determine if any found vulnerabilities have already been exploited, and reporting results to the CISO.

System/Application Administrators:

System/application administrators are responsible for, but not limited to, the following activities:

- Monitoring system integrity, protection levels, and security related events during assessments.
- Scheduling security testing in accordance with defined internals required by this procedure and coordinating with the CISO.
- Documenting and reporting assessment/test results to the CISO.
- Implementing corrective measures in accordance CISO guidelines.
- Conducting security assessments/tests in accordance with this procedure or as directed by the CISO.
- Each administrator will subscribe to credible subscription service(s) that monitors for new software vulnerabilities for applications and systems supported. In the event a high-risk vulnerability is reported, ensure the environment is scanned as soon as possible.

System/Application Owners:

System/application owners are responsible for, but not limited to, the following activities:

- Work with the CISO and, if applicable, third parties who perform assessments to ensure testing is accomplished with little to no disruption to the organization and business operations.
- Perform system/application specific assessments as defined by this procedure and if significant changes take place perform the relevant test on demand. Coordinate all assessment activity with the CISO.
- Implement approved remediation activities as soon as possible or as defined in the plan of action and milestones (POAM).

Management:
Management is responsible for providing budget and resources to support the vulnerability management program. Management will also ensure that they receive periodic briefings on the results of vulnerability management activities.

Third Party Relationships:
Third party vendors are required to maintain their own vulnerability management program to ensure covered information is properly protected against breaches of confidentiality, integrity and availability. See the Third-Party Assurance procedure.

Vulnerability Assessments:
The primary purpose of the vulnerability management program is to define the different types of assessments that will be periodically performed to proactively identify new and existing vulnerabilities that pose a threat to covered information and business operations. Due to the diverse nature of information technology, different types of assessments are required. These assessments consist of:

- Perimeter Vulnerability Assessment (PVA): PVAs attempt to determine the security of the network perimeter from the perspective of an outside attacker. PVAs consist of:
  - Profiling: Port scanning, banner grabbing, and other information-gathering techniques are used to identify active hosts and services.
  - Vulnerability Scanning: Commercial and open source scanning tools are used to identify potential vulnerabilities to include:
    - Unauthorized remote access connections
    - Unnecessary and/or non-secure functions, ports, protocols, and/or services
- Internal Vulnerability Scan (IVS): IVS will assess the security of an organization's internal network environment. The IVS will include internal network vulnerability scanning to identify anomalies such as missing patches, known vulnerabilities and configuration issues such as weak passwords, unnecessary and/or non-secure functions, ports, protocols, and/or services, etc.
- Network Security Assessment (NSA): NSAs will assess the security of network systems using applicable regulatory requirements and security best practices/frameworks as an assessment baseline. NSA includes inquiries, observation, and inspection of relevant documentation relating to the following:
  - Data processing facilities security and environmental controls
  - Controls over portable devices that connect to the network environment
  - Change management policies and procedures
  - Network documentation (e.g., inventories, diagrams, checklists, standards, procedures, and change logs)
  - Secure configuration management practices
  - Patch management process
  - Security audit logging and monitoring practices
  - Network incident response procedures
  - Fault tolerance measures and data recovery procedures
  - Processes associated with granting, revocation, and changing network access privileges
  - Methodology for granting and periodic review of network permissions and resources
  - Password management controls (e.g., password length, password age, account lockout threshold)

- Use of network segmentation, network access control (NAC), demilitarized zones (DMZs), intrusion detection/prevention systems (IDS), etc.
- Remote access management
- Effectiveness of firewall technology, including firewall policy (i.e., ruleset) review
- Anti-viral/spam protection

- Automated assessment tools will be used to evaluate the effectiveness of:
    - Identification and authentication (i.e., password) controls
        - Group security policies
        - Secure configuration guidelines
        - Active directory for:
            - Potentially rogue, dormant, generic, duplicate accounts
            - Time-of-day and workstation restrictions
            - Audit settings
            - Excessive administrator rights
            - Minimum necessary access (i.e., least privilege)
            - Appropriate separation of duty/responsibility
- Web Applications (e.g., client/patient portals, electronic commerce services, etc.): Website vulnerability assessments attempt to determine the vulnerability state of a target website and the related host or network from the perspective of an outside attacker. These assessments consist of three stages:
    - Profiling: Port scanning, banner grabbing, and other information-gathering techniques are used to identify active hosts and services.
    - Vulnerability Scanning: Commercial and open source scanning tools are used to identify potential vulnerabilities.
    - Vulnerability Analysis: Proprietary and publicly available tools and techniques are used to validate results (eliminating false positives) and identify vulnerabilities not otherwise found (false negatives) using automated scanning tools.
- Wireless Security Assessment (WSA) is an assessment of the existing wireless networks (i.e., business and guest). The objectives of WSA are to:
    - Identification of unacceptable use of wireless networks
    - Identification of misconfigured wireless network devices
    - Security patches/updates have been implemented
    - Identification of unapproved/unidentifiable (i.e., rogue) wireless access points (i.e., hotspots)
    - Validate that strong authentication and encryption are still being enforced
    - Validate logging of wireless activity is being performed in accordance with the Audit Logging and Monitoring procedure.
- Security Test and Evaluation (STandE) is an assessment of new systems/applications (acquired or internally developed). This assessment is performed before the new system/application is put into production. The objectives of the STandE are to:
    - Identify the design, implementation, and operational flaws, misconfigurations, and default settings that have not been fixed/changed.
    - Measure the effectiveness of implemented security controls.
    - Ensure that system security plans remain current (see Security Configuration Management procedure).

- Application Security Assessment: Application security assessments are designed to periodically monitor the effectiveness of security controls within existing production applications. Application security assessments require both manual processes and the use of automated tools. The objectives of application security assessments are to evaluate the effectiveness of the following:
  - Input data validation controls
  - Data integrity controls
  - Access controls
  - Logging and auditing controls
  - Secure configuration requirements
- Unauthorized Components/Devices Scan: An accepted list of components/devices (hardware, firmware, software) will be documented and kept up to date whenever changes are made. For compliance on this objective, a scan will be performed on the workforce network. This scan is to determine if there are any unauthorized components/devices installed on the workforce network. Any unauthorized components/devices found shall either be removed/have their network access disabled or evaluated against the risk management standards (See Information Security Risk Management procedure) and, if approved, added to the organization's asset listing.
- Preventative Malware Threat Assessment: On a periodic basis, information systems that are not normally affected by malicious software or that do not currently run any malicious scanning tools will be evaluated. The purpose of this evaluation is to determine if systems require more protection or in the case of a system not running any type of protection, if that is still appropriate.

Vulnerability Mitigation:

Identified assessment vulnerabilities will be documented, analyzed, prioritized, and mitigated/remediated in the most expeditious manner possible in accordance with Cone Health's risk management process (see Information Security Risk Management procedure).

Documentation:

Assessment results must be formally documented and retained for a period of no less than 6 years from the date the assessment report. Assessment documentation is often needed for the following reasons:

Documentation Retention:

Assessment documentations will be retained for a period of no less than 6 years from the date of the assessment's final report.

Exception Management:

Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are compensated by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.

Appendix 1: Assessment Schedule

Assessment Type	*Frequency of Testing
Perimeter Vulnerability Assessment (PVA)	Annually
Internal Vulnerability Scan (IVS)	Quarterly
Web Application Assessments	Quarterly
Network Security Assessment (NSA)	Quarterly
Wireless Security Assessment (WSA)	Annually
Application Security Assessment	Quarterly
Security Test and Evaluation	Pre-Production
Unauthorized Components/Devices Scan	Weekly

*Internal testing will only be performed by personnel who are authorized and properly trained on the use of the technology solutions being used.