CONE HEALTH	**Policy:** ITS Information Security Training and Awareness Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/19/2024
	Effective Date: 06/19/2024	**Next Review Date:** 06/19/2025

INTENDED AUDIENCE:
Entire workforce

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), confidential, and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits at a level which is reasonable and appropriate with the associated classification level, regardless of format (i.e., electronic, paper, voice, etc.).

The purpose of this procedure is to define Cone Health's requirements for initial, annual, and recurring security training for the general workforce, and specialized training requirements for individuals who have security related responsibilities.

Scope and Goals:
The scope and goals of the security training and awareness program are as follows:

- General Training: Formal training of workforce members upon hire/contract in the form of orientation training and on an annual basis thereafter. General training focuses on applicable information security policies/procedures, review of confidentiality/non-disclosure and acceptable use agreements. This type of training requires formal documentation that each workforce member must sign.
- Specialized Training: Formal training for workforce members who have security-related responsibilities (e.g., security administrators, security personnel, developers, etc.).
- Contingency Plan Training: To information system users consistent with assigned roles and responsibilities. This type of training requires formal documentation that each workforce member must sign.
- Awareness Training: Informal training meant to keep the workforce informed of current threats, preventing bad practices, short policy reminders, etc. Members do not need to acknowledge receipt of awareness training.

Responsibilities:
Chief Information Security Officer:
Cone Health's chief information security officer (CISO) is responsible for maintenance, interpretation and enforcement of this procedure. Additional responsibilities include, but are not limited to, the following:

- Ensure newly hired/contracted personnel are provided information security training prior to being given access to covered information or any system that processes it.

- Ensure newly hired/contracted personnel sign the confidentiality/non-disclosure, acceptable use and other agreements, as applicable, to their job responsibilities.
- Ensure the entire workforce (including contractors) is provided initial training within 60 days and annual training every year afterwards that includes a review of applicable information security policies/procedures, and a review/re-sign of confidentiality/non-disclosure, and acceptable use and other agreements, as applicable, to their job responsibilities.
- Ensure workforce, as applicable to assigned roles, is provided contingency plan training within ninety (90) days of assuming an incident response role or responsibility, when required by information system changes, and annually thereafter.
- Ensure personnel assigned security-related responsibilities are getting professional training on an annual basis.
- Ensure that records are kept for any general or specialized training a workforce member completes for at least 5 years.
- Ensure that senior management receives all standard training and any relevant specialized training related to their position within the organization.

Management:

Management is responsible for ensuring the workforce receives required security training and provide sufficient funding to support the requirements in this procedure.

Awareness Program Content:

Security awareness topics will be based upon the following areas. Each of these topics will be addressed using the deployment methods described below. Due to changing business and regulatory requirements, new or changing policies, new threats or risks, etc., topics will periodically be added, removed or modified to adjust for organizational need:

- Organizational Security Policies and Procedures
- Acceptable Use of Information Technology and Services
- Social Engineering
- Command Center and Incident Management (Crisis Management) Awareness
- Fire Safety
- Access Control and Rights
- Identity Theft
- Physical Security
- Perimeter and Facility Alarm Response
- Information Classification and Handling
- Password Creation and Management
- Virus/Hoaxes/Spyware/Spam/Malicious Software
- Regulatory Issues (HIPAA, PCI, etc.)
- Use of Social Media
- Privacy Expectations While Using Cone Health Resources
- Teleworking/Working Remotely
- Incident Identification and Reporting
- Contingency Plan (consistent with roles)
- Mobile Device Security

- Insider Threat
- Sanctions/Disciplinary Action for Non-Compliance with Security Policies/Procedures
- Personal Device Use in the Workplace
- Approved Software that Can be Installed on Organization's Computers
- Remedial Type Training Associated in Lessons Learned from Security Incidents, Breaches, Audits, and Compliance-Related Activities.

Methods for Delivering Security Awareness Training:
Techniques for delivering and promoting information security awareness are:

- Information Security open house events
- A web-based or in person new hire training
- Periodic company newsletter announcements
- Posters and signs strategically placed around the organization
- Notices describing the responsibilities of the associates are posed during logon
- Quarterly Information Security newsletters
- Email notifications
- Department meetings
- Corrective training following an information security incident
- Security messages within system banners
- Screensaver messages
- Awareness messages on marketing type giveaways (e.g., pens, Post-It Notes, mouse pads, etc.)
- Instructor led presentations
- Brown-bag presentations
- Awards program
- Video presentations
- Partnering with Privacy, Ethics, People and Culture, Compliance, etc., to create one-stop training

Specialized Training Requirements:
Specialized training is achieved by attending professional conferences/courses, college/trade classes, etc. Specialized training can also be achieved through webinars, vendor presentations, attending professional trade groups, etc., which is considered supplementary training and not a substitute for attending formal in-person conferences, courses and classes. Specialized training is meant to keep members up to date on security technology, security best practices, changes to regulatory requirements, and current and future threats. Members who perform security functions will attend at least one type of specialized training on an annual basis, in addition to supplementary training.

Evaluation and Feedback:
On an annual basis, the CISO will use formal evaluation and feedback mechanisms to measure the effectiveness of the training and awareness program. Evaluation and feedback mechanisms will include surveys, evaluation forms, independent observation, status reports, interviews, focus groups, and benchmarking to provide continuous improvement of the program. Based on the outcomes from this evaluation, the training and awareness program will be reviewed and updated as needed.

The feedback strategy shall incorporate elements that will address quality, scope, deployment method (e.g., web-based, onsite, offsite), level of difficulty, ease of use, duration of session, relevancy, currency, and suggestions for modification

Documentation Retention:
Previous versions of this procedure and training documentation will be retained for a minimum of 6 years.

Exception Management:
Exceptions to this policy/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 directly compensated for services/work 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.