CONE HEALTH	**Guideline:** ITS Teleworking Security 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:
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.

The purpose of this procedure is to define administrative, technical, and physical security requirements to be taken by authorized team members when working from home, while traveling, or at any location not owned by Cone Health.

Scope and Goals:
This procedure pertains to all situations when authorized team members are working abroad/teleworking. The goals of this procedure are as follows:

- Define roles and responsibilities for compliance and enforcement of this procedure.
- Establish administrative, technical, and physical security requirements for team members working remotely.

Responsibilities:
Chief Information Security Officer:
The chief information security officer (CISO) is responsible for overall enforcement and interpretation of this procedure and educating authorized team members of their responsibilities as outlined in this procedure.

Team Members:
Team members' job responsibilities do not change when teleworking. Professionalism, ethical behavior, adherence to the organization's policies, work output expectation, and client/customer services will be maintained in accordance with Cone Health standards. Team members are required to have their leader's approval prior to working offsite.

Leadership:
Leaders will consider the following when approving teleworking activities:

- Definition of work permitted to be performed when teleworking.
- Hours of work (if applicable).
- Classification of information that may be held.
- Internal systems and services the teleworker may access.
- If additional insurance is needed to address the risks of teleworking activities.

Administrative Security Requirements:
Teleworkers will abide by the following administrative security requirements:

- Only Cone Health owned computers will be used when working with covered information, unless the device has been approved by the individual's manager, the CISO, and complies with the requirements outlined in Cone Health's Personal Device Use procedure.
- All covered information will be accessed and maintained on the Cone Health network, system or application. Do not store covered information on mobile devices or portable media unless approved by the CISO. If approved, only mobile devices and portable media utilizing hard-drive encryption will be used.
- Ensure you are connecting to legitimate public Wi-Fi networks by asking business owners or someone who would know, what the official network name and password is.
- Hardcopy covered information will be shredded beyond reasonable reconstruction or brought into office and disposed of in Cone Health's secure shredding containers when no longer needed.
- Team member will comply with security requirements contained in the Information Technology Acceptable Use procedure

Technical Security Requirements:
The use of public/shared networks (i.e., wireless, hotel wired, etc.) can expose users to the possibility of a host of security risks (i.e., interception of communications, unauthorized access to your computer, etc.). When using public/shared networks, Cone Health teleworkers will comply with the following technical security requirements:

- Utilize multi-factor authentication when remotely accessing internal Cone Health resources.
- Enable a password locked screensaver. Ensure it requires your password to re-access the computer.
- Utilize data encryption techniques when transmitting covered information (i.e., VPN, SSL, TLS, secure email, etc.).
- Utilize hard-drive encryption when storing data on mobile devices or portable media.
- For wireless networks, AES WPA2 encryption at a minimum must be used.

Physical Security Requirements:
Team members will abide by the following physical security requirements:

- Ensure their immediate work environment is free of security risks that could result in unauthorized access (e.g., view, copy, print). Examples of physical actions to take include, but are not limited to, the following:
    - Working in a room where access can be controlled or people entering the area can be seen (e.g., office).
    - Positioning the computer screen/monitor in a manner that covered information cannot be inadvertently or intentionally read by unauthorized personnel.
    - Use of a computer privacy screen.
    - Not working with covered information in public places (e.g., on plane, in airport, coffee shops, plane, train, etc.).
- Hardcopy covered information not in use will be secured in a manner to prevent unauthorized access.

- When working from home, family members, house guests, friends, relatives, etc., will not be allowed to use computers owned by the organization or personal computers authorized to be used for work related purposes.
- Never leave an approved work computer unattended. Take the computer with you, or if this is not possible, log out of the system, application, and network, and then turn off the computer or enable the password locked screensaver to prevent unauthorized access.
- Take appropriate steps to properly protect all portable electronic media (e.g., CD-ROMs, flash/thumb drives, etc.) containing covered information from unauthorized access or theft.

Traveling to High-Risk Locations:
Before traveling overseas or to other areas identified by the organization as being high-risk, team members will contact ITS to determine if any additional physical or technical security controls are required. Upon return from a high-risk location, team members will check in with ITS so that they can perform a security check of the device to ensure it has not been tampered with or contains malicious software.

Documentation Retention:
Retain copies of signed teleworking agreements (e.g., signing of the Information Technology Acceptable Use procedure) for a minimum of no less than 6 years.

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., team members) 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:
Team members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Team members who fail to abide by requirements outlined in information security policies/procedures may be subject to corrective action up to and including separation of employment/termination of contract.