CONE HEALTH	**Guideline:** ITS Wireless Network Security 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), sensitive, and confidential data (hereafter all three will be referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes associated with the management of wireless networks used to transmit covered information.

Scope and Goals:
This procedure applies to wireless networks managed by Cone Health or third-party service providers on behalf of the organization. The goals of this procedure are as follows:

- Define security requirements for business and guest wireless networks.
- Define auditing and monitoring requirements for wireless networks.
- Define security requirements for teleworkers who work from home.

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.
- Defining and documenting wireless security configuration management requirements.

Information and Technology Services (ITS):
ITS is responsible for, but not limited to, the following activities:

- Maintain a secure environment for both business and guest wireless networks in accordance with this procedure.
- Maintain an inventory of authorized wireless access points.
- Approve or deny the installation of new wireless access points.
- Implement and maintain the secure configuration requirements defined by the CISO.
- Monitor security of the wireless networks.
- Conduct periodic assessments (see Vulnerability Management procedure) to detect unauthorized access and malicious activity.
- Conduct quarterly scans to identify any unauthorized wireless access points and take appropriate action if any are discovered.

- Ensure that wireless access points are disabled when not in use (e.g., nights, weekends).

Wireless Network Access:

Business Wireless Network:

Access to the business wireless network will be based on role and job responsibility (i.e., need to have). Access will be limited to organizationally owned devices. Personally owned devices will not be allowed to access the business wireless network unless they have been approved by management and the CISO. These devices must also meet the security configuration requirements defined in the Personal Device Use and Security Configuration Management procedures.

Business wireless network access management will be conducted in the same manner as any other Cone Health's system/application. Access management requirements are defined in the Information Access Management procedure.

Business wireless networks will be physically and logically separated from non-business related (i.e. guest) wireless networks.

Guest Wireless Network:

Provided all requirements are implemented for guest wireless configuration and infrastructure segmentation (as defined in this procedure), unauthenticated access to the guest wireless is allowed. Guest wireless networks must comply with the following security requirements:

- Will not be used to transmit covered information.
- Will prompt users accessing the network to read and accept a Terms of Use Agreement. Users will be prompted to read/accept these terms every 24-hour period. Terms of Use Agreement language will be defined by Cone Health's general counsel who will ensure that the agreement contains the appropriate language and does not violate any federal or statutory requirements.
- Will be limited to only internet access.

Audit and Monitoring Wireless Activity:

Business Wireless Network:

Auditing and monitoring wireless activity will comply with the requirements outlined in the Audit Logging and Monitoring procedure, in addition to the following:

- Authorized and unauthorized users/devices attempting to access or currently connected to the network.
- Malicious or suspicious activity such as denial of service attacks, rogue access points, virus patterns, failed access attempts, attempts to change or circumvent security requirements, etc.
- Failed and successful authentication.
- Date, time, and user identification for all successful or unsuccessful access attempts.

Guest Wireless Network:

The guest wireless network activity will be periodically monitored for excessive bandwidth use and malicious or inappropriate activity. Audit logs will record the date and time of access and device identification (i.e., media access control [MAC] address).

Wireless Network/Device Security Requirements:

Business Wireless Network:

At a minimum, the business wireless network will be configured as follows:

- Auditing enabled to ensure that all activity will be traceable to an individual (i.e., workforce member).
- Broadcasting service set identifier (SSID) will be disabled.
- Limit the range of reception to reduce signal from being intercepted in areas not controlled by Cone Health (e.g., outside of the building, parking lot, etc.).
- Each wireless network will have their own unique SSID.
- Implement AES WPA2 encryption.
- Implement strong authentication (EAP, LEAP, PEAP, EAP-TLS, and EAP-TTLS). Open authentication IS NOT allowed under any circumstances.
- Implement MAC address access control or some other form of device identification.
- Network management traffic intended for access points will be over a dedicated wired subnet utilizing secure protocols (e.g., SSL, SSH, SNMPv3, etc.).
- Password management and composition (e.g., user, administrative, and service accounts) will comply with the Identification and Authentication procedure
- Wireless device configuration will comply with the Security Configuration Management procedure.
- Be disabled when not in use (e.g., nights, weekends).
- Manufacturer default attributes will be changed to comply with Cone Health security requirements before placing any wireless technology into production. This includes, but is not limited to the following:
    - Renaming the default SSID to something unique and not easily guessable.
    - Changing administrative/service account passwords/passphrases.
    - Changing default simple network management protocol (SNMP) community strings.
    - Changing encryption keys.
    - Disable all non-essential and insecure protocols.
    - Updating the firmware to support strong encryption for authentication and transmission over the wireless network.

Endpoint Devices:

Endpoint devices will be configured as follows:

- Mobile devices must comply with the configuration standards defined in the Security Configuration Management procedure.
- Personally owned devices must comply with the Personal Device Use procedure.

Network Infrastructure:

Business Wireless Network:

The business wireless network will have its own dedicated firewall. When feasible and warranted (based on a formal risk analysis) an intrusion detection system or intrusion prevention system (IDS/IPS) will be implemented for the business wireless network.

Guest Wireless Network:

The guest wireless network will be logically separated from the business wireless network, to include virtual local area network (VLAN) environments. The guest wireless network will be configured as follows:

- Broadcasting of the service set identifier (SSID) will be enabled.
- Limit the range of reception to reduce signal from being intercepted in areas not controlled by Cone Health (e.g., outside of the building, parking lot, etc.).
- Rename the default SSID to something easily identifiable such as “Cone Health Guest Wi-Fi.”
- Will prompt users accessing the network to read and accept a Terms of Use Agreement.
- Limited to only internet access.

Physical Security Requirements:

Wireless device management systems will be physically secured in a data closet or other means that restricts tampering and unauthorized access. The supporting wireless access points will be secured in a manner to prevent tampering.

Home Wireless Networks:

For workforce members who are allowed to work from home and the work being performed could involve access to covered information, every attempt will be made to ensure that the home user is made aware of their responsibility for physically and logically securing their home wireless network. This includes using wireless encryption of AES WPA2 at a minimum. Home wireless network use that could involve the transmission of covered information must be approved by the CISO and only after performing a formal risk analysis, approved by the organization’s designated approving authority.

Documentation Retention:

Business and guest wireless networks will be documented and maintained for future reference (e.g., audits, assessments, disaster recovery, etc.). At a minimum, documentation will include the following:

- Wireless network infrastructure diagram that shows the location of all devices, access points, etc.
- Wireless network component inventory.
- Security attributes and configuration standard.
- Identification of personal devices used to access the business wireless network.
- Identification of home wireless networks used to transmit covered information.

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.

Guideline: ITS Wireless Network Security Procedure

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.