CONE HEALTH	**Guideline:** ITS Network 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:
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 roles, responsibilities, and processes associated with creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.

Scope and Goals:
The procedure addresses network security management requirements (e.g., policy, process, and technology) required to protect the organization's network infrastructure, services, and resources against unauthorized access and to ensure that the workforce has adequate access to fulfill their job responsibilities. The goals of this procedure are as follows:

- Define authorized use of network services and resources.
- Define firewall management requirements.
- Define network segmentation requirements.
- Define network security controls required by the organization.
- Define requirements for external connectivity to the network.
- Define encryption key management requirements.
- Define physical and environmental controls related to the network.

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.
- Review and approve firewall rule change requests.
- Ensure all formal agreements with network service providers (e.g., contracts, service level agreements, memorandum of agreement) include specific obligations for security and privacy requirements (including the right to audit), service levels, and management requirements.

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

- Implementing and maintaining network security controls in accordance with this procedure.

- Maintaining a network diagram, to include wired and wireless networks, and updating the diagram whenever there are network changes.
- Regardless if there are network changes or not, reviewing the network diagram at least once every 6 months to ensure accuracy.
- Firewall, router, switches, and network connection changes will be tested and approved by the appropriate authority prior to implementation.
- Manage and monitor approved network services to ensure they are being provided securely.
- Ensure enterprise architecture design and maintenance continually provides consideration for information security.
- Perform quarterly network scans to identify any unauthorized components or devices connected to the network and take appropriate action when discovered.
- Ensuring router configuration files are secured and synchronized (start-up file and running configuration must match up).
- If for some reason, a dial-up network is required, ensure the connections are encrypted. If the connection cannot be encrypted, approval must be obtained from management to implement. Also, for all dial-up connections, ensure that a callback mechanism is in place with re-authorization to verify the dial-up connections are coming from an authorized location.

Firewall administrators are responsible for, but not limited to the following activities:

- Maintenance and overall management of Cone Health's firewall architecture.
- Monthly review of firewall access control list (ACL).
- Twice a year, reviewing the firewall and router configuration standards.

Business Leaders:

Business leaders are responsible for, but not limited to the following activities:

- Work with ITS to define network services needed to perform business functions.
- Formally define the impact that the loss of network service would mean to the business.

Application/System Owners:

Application/system owners are responsible for, but not limited to, the following activities:

- Identifying and documenting the sensitivity and criticality of the applications/systems they are responsible for.
- Formally authorize and document the characteristics of each connection between the internal network and external network locations (i.e., customer and vendor networks). These connections and written agreements must be reviewed on a periodic basis.
- Develop and maintain unique information security architecture documentation for every application/system they are responsible for. Review and update architecture documentation whenever changes occur.

Network Protection:

Use of Network Services:

The organization ensures network services are properly allocated/assigned and individuals are limited to only those services they require to perform their assigned responsibilities. Network administrators

will work with business leaders to develop and maintain a list of services, ports and protocols, means of access, justification for service and a list of authorized users for each.

External Connectivity:
ITS, with the assistance of business leaders, will identify, authorize, and manage all external information systems used by the workforce (i.e., instant messaging, Dropbox, cloud storage, etc.). Workforce members will be prohibited from using external systems until the CISO and ITS can verify that appropriate security controls are in place.

Network Segregation:
Firewalls will be used to enforce logical access control:

- Between internal system (wired and wireless) connectivity, external systems, and any demilitarized zones (DMZ).
- Internally between covered environments (i.e., systems containing covered information) and non-covered environments (i.e., guest and business wireless networks).
- For each network access point or external telecommunication service managed interface.
- Between physical and virtualized servers when migrating applications or data.

The organization's network will be logically and physically segmented with a defined (i.e., documented) security perimeter and controls, including sub-networks for publicly accessible system components that are logically separated from the internal network as defined by organizational requirements. Network traffic will be controlled based on functionality required and data classification standards.

ITS will maintain current network and data flow diagrams for all approved systems used and managed by Cone Health. The network diagram identifies all high-risk environments, data flows, and connections to systems storing, processing, or transmitting covered information.

Network Connection Control:
The ability to connect to the internal network is restricted using a deny-by-default and allow-by-exception policy at managed interfaces in accordance with the organization's Information Access Management policy and requirements of the business applications.

Exceptions to any of the network security requirements stated in this procedure will be documented and include the business need and duration for the exception. If an exception surpasses a year in length, it will be reviewed on the anniversary of the approval date to determine if the business need still supports the exception decision, or if there are other alternates that would allow for the exception to be eliminated. Exceptions that are no longer supported by an explicit business need will be terminated.

Network Routing Control:
Network routing control will be performed by the organization's firewall for communications between internal resources and external networks. The firewall will validate source and destination addresses and hide internal directory services and internet protocol (IP) addresses from unauthorized viewing and manipulation.

Sensitive System Isolation:
Sensitive systems will be physically and logically (both through firewall rule configuration and minimum necessary access control) isolated from non-sensitive applications/systems unless the risk of cohabitation is identified and accepted by the application/system owner and the organization's designated approving authority (DAA).

General Network Security Controls:
The following general network security controls will be implemented and maintained by Cone Health:

- All remote devices will be required to uniquely identify (i.e., IP or MAC address) and authenticate (i.e., access control) before establishing a connection to the network.
- All outbound network transmissions that will be sent over open, public networks, will be encrypted.
- Firewalls will restrict inbound and outbound traffic to the minimum necessary.
- Technical security tools (e.g., intrusion detection/prevention system) are operating on the network perimeter and other key points to identify vulnerabilities and mitigate threats, and are updated on a regular basis.
- Public-facing web applications are required to have an application-level firewall implemented as a secondary level of controlling traffic. For public-facing applications that are not web-based, a network-based firewall specific to the application type will be deployed. If the traffic to the public-facing application is encrypted, the device either sits behind the encryption or is capable of decrypting the traffic prior to analysis.
- Utilize a filtering proxy for all outgoing network traffic to the internet. The proxy will be used to enforce controlled internet access, allowing users to connect to only approved sites and block known malicious or unapproved sites.
- Deny all access to proxies, except for those hosts, ports, and services that are explicitly necessary.
- Utilize firewalls from 2 different vendors that employ stateful packet inspection.
- Establish a DMZ (also known as a perimeter network) and place all databases, servers, and other system components storing or processing covered information behind it to limit external network traffic to the internal network.
- Utilize at least two DNS servers that are located on different subnets, are geographically separated, and perform separate roles (internal and external) to eliminate single points of failure and enhance redundancy.

Encryption Key Management:
The following security requirements will be implemented and maintained for Cone Health's encryption key management:

- Encryption key management is implemented based on specific roles and responsibilities and in consideration of national and international regulations, restrictions and issues.
- Where a certificate authority is used (e.g., for the purposes of issuing and maintaining digital signatures and/or digital certificates), security is integrated and embedded throughout the entire end-to-end certificate/signature management process. This includes:
    - Ensuring that only approved certificate authorities are used.
    - Management of the certificates is limited to only approved workforce members.

  - Certificates are stored securely.
  - Access to the certificates is given only to those workforce members that require it.
- Encryption keys will not be stored in the cloud in plain text.
- If encryption keys are stored in the cloud, then it must be through the use of a trusted key management platform.
- Encryption key management and key usage duties will be separated between workforce members.

Server Migration:
The following security requirements shall be followed when migrating data between servers including on-premise, virtualized, or between the two types:

- A secure transmission method utilizing the encryption level standards outlined in Cone Health's Data Classification and Handling and Security Configuration policies/procedures.
- Network segregation (defined above).

Environmental:
An uninterruptable power supply (UPS) is required for all network equipment supporting critical business operations to support a controlled power down of equipment or transfer to another power source (i.e., generator).

UPS and generators will be regularly (i.e., monthly) checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations. Administrators will plan for contingency operations should a UPS fail (i.e., manual transfer to backup generator).

Physical Security:
The following physical security requirements will be implemented and maintained for Cone Health network resources:

- Ensure network equipment is protected against unauthorized access, interception, damage, and tampering.
- Ensure power and communications cabling are properly segregated to prevent interference when copper communications cables are used.
- Maintain a documented patch list and clearly identifiable cable/equipment identification to minimize handling errors, such as accidental patching of wrong network cables.
- Limit access to patch panels, information system distribution, transmission lines, and cable rooms in accordance with minimum necessary requirements.
- Disable any physical ports (e.g., wiring closets, patch panels, etc.) not in use and implement physical/logical access controls to restrict access to publicly accessible network jacks.
- Routers, switches, servers, firewalls, etc., physically located in areas that cannot be properly protected against tampering or are in areas that are shared by other tenants of a building, will be physically locked in an approved security cabinet. Data and electrical cabling will be protected in a manner that prevents tampering, unplugging, etc. This equipment will be randomly checked and recorded at least once daily by appropriate ITS personnel facility security or facility maintenance. Under no condition will keys to cabinets be left unattended in the cabinet lock.

Additional guidance can be found in the Facility and Environmental Security Management procedure.

Firewall Management:

Access Control:

Access to Cone Health's firewalls will be limited to only those individuals who have administrative responsibilities.

Remote access to firewalls will be for maintenance and management purposes only. Remote connectivity will only be performed over encrypted channels (e.g., SSL, VPN, etc.) and using multi-factor authentication.

Firewall devices will be physically secured in the data center or a locked data closet with appropriate access controls.

Change Management:

Preventative maintenance changes to firewalls do not require Change Advisory Board approval, provided the maintenance is at preapproved intervals or are part of scheduled downtime periods. Major configuration changes to the firewall will require formal CAB approval (see Change Management procedure)

Firewall Policy Rules:

Requests to change or modify existing firewall policy rules (temporary or permanent) will be reviewed with and approved by the CISO before submitting to the CAB. The CISO will perform a risk analysis (see Information Security Risk Management procedure) to determine if the change will result in unacceptable risk(s) to the organization.

Firewall rules will be reviewed by firewall administrator(s) and the CISO on a quarterly basis. Changes will be made accordingly.

A backup copy of firewall policy rules will be retained for contingency purposes and used for quarterly policy reviews.

Firewall administrators will maintain a log of all firewall policy rule changes. The log will contain the following information:

- Requestor name, email address and phone number
- Date change took place
- Reason/justification for request

Configuration Management:

Patches or upgrades that mitigate vulnerabilities or correct performance issues will be implemented as soon as possible (see Security Configuration Management).

Configuration of firewalls will be based upon National Institute of Standards and Technology (NIST) Special Publication 800-41, Guidelines on Firewalls and Firewall Policy and vendor's security configuration standards (see Security Configuration Management procedure).

Vulnerability Management:
Vulnerability assessments of firewalls and network perimeter will be performed in accordance with Cone Health's Vulnerability Management procedure.

Audit Requirements:
Firewall audit logs will be configured to record the following:

- Date and time of all access attempts
- Internet protocol (IP) address of resources (i.e., source address/identifier) accessing or attempting to access Cone Health resources, to include destination address
- All successful/unsuccessful attempts to access internal/external Cone Health resources
- Attempts to circumvent the firewall
- Administrative level changes (e.g., change in privileges, security attributes or access controls, etc.).
- Identification of all services and ports accessed, to include date, time, source address/identifier, etc.
- The individual responsible for firewall administration will review their audit logs daily for any suspicious activity. Suspicious activity will be brought to the attention of the CISO for action.
- See Cone Health's Audit Logging and Monitoring procedure for additional requirements and log retention requirements.

Contingency Planning:
Firewall configuration(s) will be included in the ITS disaster recovery plan.

Architecture:
Firewall topology will be documented in Cone Health's network diagram.

Documentation Retention:
Audit logs shall be maintained based on organizational needs. For the purpose of HIPAA compliance, reports summarizing audit activities shall be retained for a period of six years. Retention of audit logs shall be based on:

- Organizational history and experience
- Available storage space
- Regulatory and legal requirements
- Organizational records retention policy

Audit logs that are retained will be:

- Backed-up as part of the application's regular backup process.
- Periodically audited by the security officer for availability and integrity purposes.
- Retained for 90 days on the production server, then archived for 1 year, unless otherwise instructed by People and Culture, legal counsel or other entity (i.e. evidence, investigation, etc.).

Systems will shut down and stop generating audit logs or overwrite the oldest records first, should storage media (i.e., hard drive) become unavailable. An alert will be sent to the designated personnel for any audit processing failure.

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.