CONE HEALTH	**Guideline:** ITS Facility and Environmental Security Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 02/14/2024
	Effective Date: 02/14/2024	**Next Review Date:** 02/14/2025

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 roles, responsibilities and processes associated with physical/facility security.

Scope and Goals:
The scope of this procedure pertains to visitor control, maintenance and construction requirements. It also covers physical security requirements for areas such as the data center, telephone/data closets, workstation staging/storage areas, generator room, HVAC room, electrical closets, emergency room, laboratory, patient care areas, pharmacy, asset storage, cabling, records room, loading docks, etc.
Goals of this procedure are as follows:

- Workforce identification requirements
- Define requirements for areas defined as “restricted”
- Define maintenance requirements for physical security and environmental facility controls
- Define construction requirements for areas requiring an elevated level of physical security
- Define visitor control requirements
- Define emergency personnel access

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.
- Work with Facilities Management to identify and formally document all restricted areas.
- Maintain a list of all individuals who have access to each restricted area.
- Perform a monthly review of the visitor control log for discrepancies.
- Ensure a history of at least 2 years is maintained for visitor logs.
- Approve all structural modifications and repairs to restricted areas to ensure that the appropriate security controls are implemented or remain in place.
- Maintain a list of authorized maintenance organizations and/or personnel, ensure that non-escorted personnel performing maintenance have required access authorizations, and designate organizational personnel with required access authorizations and technical competence to

supervise the maintenance activities of personnel who do not possess the required access authorizations and ensure that non-escorted personnel performing maintenance have required access authorizations.
- Work with facility management to ensure that fire suppression systems (e.g., extinguishers within 50 feet of critical equipment, sprinkler system, chemical retardant, etc.) and detectors are installed and tested in accordance with applicable laws and regulations.
- Ensure that the fire suppression systems are configured to automatically notify the fire department in the event of a fire.
- Review general physical access rights every 90 days and update the appropriate person or mechanism based on findings.
- Ensure an audit trail is being maintained for all physical access within Cone Health facilities and restricted areas.

Facilities Management:
Facilities Management is responsible for, but not limited to, the following activities:
- Perform monthly preventative maintenance on all physical security devices.
- Periodically test all facility alarms to ensure they are operating as intended.
- Maintain an electronic log of all alarm system events and review the log for any outstanding issues monthly or on demand if necessary.
- Ensure all areas designated as "restricted" comply with construction requirements outlined in this procedure.
- Take inventory of all physical access devices every 90 days.
- Maintain an inventory of all physical keys to restricted areas and perform a semi-annual audit of all physical keys.
- Change locks, re-key doors, etc., when appropriate (i.e., terminations, lost key, etc.).
- Ensure fire suppression and detection systems are supported by an independent energy source.

Business Units:
Business units that include restricted areas are responsible for, but not limited to, the following activities:
- Perform a quarterly review of the restricted areas access control lists to ensure all personal with access is still appropriate.
- Promptly retrieve keys or badges from terminated workforce members.
- Perform a quarterly review of system audit logs containing restricted area access (e.g., proximity/swipe cards, security cameras, etc.) to identify abuse or unauthorized attempts to access restricted areas.
- Approve and manage access to restricted areas.
- In the event of a compromise, inform Facilities Management there is a need to change or rekey locks.

Workforce Identification Badges:
All personnel will be issued their own identification badge that will be used to identify them as a member of Cone Health's workforce.

Third party entities who come onsite to perform contractual duties for the organization, who are the same individual(s), have had a background check and are bonded by their organization, and evidence of such has been provided to Cone Health, can be issued their own identification badge. Badges will be turned in when departing a Cone Health facility and can be picked up when the third-party entity returns.

However, if these requirements are not met, then third party entities are subject to background checks based on Cone Health's Employee policy and Personnel Security Management policy/procedure.

Restricted Areas:
A restricted area is defined as any location that requires additional security to limit access to only those people who are properly authorized (i.e., minimum necessary). Restricted areas have doors and windows (if applicable) that are always locked when the area is unattended. Access will never be granted for convenience or based on an individual's authority.

The following security requirements apply to all restricted areas:

- Doors will be equipped with electronic locks and door delay alarms, will be set to lock automatically, and will never be propped open unless for environmental or work-related reasons, in which case the area will be occupied at all times by an authorized individual.
- Security alarms are optional for times when restricted areas are not manned. If alarms are used, real-time (24x7x365 security service) monitoring is required.
- Locks or devices that require the input of a specific combination of numbers and/or letters to disengage/unlock the device will be changed when:
    - Someone with knowledge of the combination terminates employment with Cone Health.
    - When the combination code becomes known by someone not authorized to have it.
    - When the lock has been worked on by a locksmith.

Under no circumstances will restricted areas be used for any other purpose, other than what they were designed or designated for (e.g., data closets being used for storage or by janitors).

Restricted areas may require additional perimeter controls such as a security fence, secondary access control, physical barriers, etc., depending on the organizational resource that is being protected. Additional security controls will be considered on a case-by-case basis.

Cameras:
Security cameras are optional and will be used if identified risks warrant monitoring activity within a restricted area, when needed to supplement other security controls, or as deemed appropriate for safety reasons. Security camera activity will be reviewed on a regular basis to detect malicious or inappropriate activity. Real time monitoring is preferred when appropriate.

Facility Alarm System:
Intrusion detection systems (e.g., alarms and surveillance equipment) are installed on all external doors and accessible windows, and at access points to restricted areas. These systems are monitored, and incidents/alarms are investigated promptly.

Key Management:
The use of proximity badges is the Cone Health's preferred method of physical access management, however, when traditional keys must be used, the following rules apply:

- Building keys will be safeguarded against unauthorized use or reproduction.
- Keys will be inventoried semi-annually by Facilities Management.
- Keys will have the words "DO NOT DUPLICATE" stamped on them.
- Restricted areas that utilize card access systems will have a physical key override for emergency access. Keys will be controlled by Facilities Management.

Shared Areas:
External organizations requiring unescorted access to restricted areas owned by Cone Health are required to comply with this procedure.

Cone Health personnel requiring unescorted access to external organizations' restricted areas will be expected to comply with that organization's physical security requirements.

Cone Health owned equipment (e.g., modems, switches, routers, servers, etc.) physically located in areas not controlled by the organization or if outside of a restricted area will be secured inside lockable cabinets to prevent tampering. Keys to these cabinets will be removed and not left in the cabinet door for convenience.

Visitor Control:
All Cone Health facility visitors are required to sign-in at the front desk of each facility. Sign-in will be accomplished through the use of a visitor control log. Upon signing in, visitors will be required to be escorted by a Cone Health workforce member. Visitors are required to wear a visitor badge in a manner that is visible while they are in a Cone Health facility. Departing visitors will be escorted back to the front desk to turn in their visitor badge and sign out on the visitor control log.

Visitor control logs must capture the following information per visitor:

- Name and organization of the person visiting.
- Signature of the visitor.
- Form of identification.
- Date of access.
- Time of entry and departure.
- Purpose of visit.
- Name and organization of person visited.

After-hours visitor access will be preapproved by the CISO. After-hours visitors (to include vendors, maintenance personnel, etc.) will always be escorted by a workforce member.

For visitors approved for unescorted access to the facility, the specific areas to which they have been authorized are documented. In addition, visitors with approved unescorted access must be issued instructions on the security requirements and emergency procedures for all areas to which they have access to.

Restricted Area Construction Requirements:
New construction and modifications to existing restricted areas must be pre-approved by the CISO and chief privacy officer and should be documented. Construction requirements for restricted areas are as follows:

- Doors will be constructed of solid core wood or metal.
- Doors will be self-closing and automatically lock.
- Exterior walls surrounding controlled areas will run from floor to ceiling to prevent anyone from climbing over the wall to gain access.
- Where appropriate, water detection mechanisms are in place with master shutoff or isolation valves accessible.
- Areas containing electrical equipment, telephone wall fields, etc., will utilize a dry pipe sprinkler system, specially rated fire extinguishers, or an inert gas system (i.e., FM200). Fire suppression will be installed according to applicable laws and regulations.
- Restricted areas will be configured with emergency lighting, surge protection, and a backup power supply (i.e., generator).
- Where applicable, a master power switch and emergency power-off switch will be installed and located near main and emergency exits. The emergency power-off switch will be protected from accidental activation.

Maintenance:
The following security rules apply to facility and security control maintenance activities:

- Maintenance activities will be conducted by properly authorized personnel and in accordance with vendor-recommended intervals, insurance policies, and Cone Health's facility maintenance program.
- Tools used by maintenance personnel (internal or third party) will be approved, controlled, monitored, and periodically checked to ensure that they are appropriate for the work being done.
- Covered information shall be cleared from any equipment (e.g., printers with data in memory) prior to maintenance or repair.
- All documentation related to maintenance will be retained in accordance with the organizational retention standard.
- Any maintenance that requires the use of diagnostic software will be checked for malicious code prior to use.
- After maintenance has been completed, all relevant security controls shall be checked and confirmed to be operating properly (i.e., if a door to a restricted area had maintenance, confirming that the automatic locks and card-based access system are still operating once maintenance has been completed).
- All maintenance and diagnostic activities will be performed locally unless it is not possible or economically feasible. In the event that remote access is required for a maintenance vendor, the access needs to be approved and all documented policy/procedure standards must be followed (See Information Access Management procedure).

Emergency Personnel Access:
Access to Cone Health facilities and restricted areas will not be denied to emergency personnel (e.g., police, firefighters, medical personnel, etc.) in the event of an emergency.

Documentation Retention:
Documentation related to repairs (e.g., restricted areas, security mechanisms, etc.), inventories, and visitor logs will be maintained for a minimum of 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., 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.