CONE HEALTH	**Guideline:** ITS Personnel 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), sensitive and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this policy/procedure is to define roles, responsibilities, and processes associated with personnel security management.

Scope and Goals:
This procedure addresses the process of ensuring workforce members hired/contracted by the organization do not bring undue risk or harm into the workplace. The goals of this policy/procedure are as follows:

- Categorize positions as they relate to periodic reinvestigations.

Responsibilities:
Chief Information Security Officer (CISO):
The CISO is responsible for, but not limited to, the following activities:

- Revision, implementation, workforce education, interpretation, and enforcement of this policy/procedure.
- Annual revalidation of position risk designations.
- Documenting all employees and their roles/responsibilities within the organization.
- Ensure security roles/responsibilities are specifically defined (in writing).

Third Party:
Third party relationships such as business associates, vendors, contractors, consultants, etc., will be required to abide by the requirements outlined in this policy/procedure under the terms of their contract with Cone Health. Third parties will be responsible for performing their own background investigations and providing results to Cone Health, if requested.

Background Checks:
Refer to the Employment policy for information on the formal background check process.

Adverse Action:
Refer to the Employment policy for information on adverse employment action.

Guideline: ITS Personnel Security Management Procedure

Position Categorization:
All Cone Health positions will be assigned a "risk" designation level of Minimum, Moderate, or High. Risk designation will be assigned according to the following criteria:

- Minimum Risk: Positions where responsibilities do not provide access to systems used to manage covered information (physical or electronic) or a permission level required to manage covered information. Examples of positions/areas in this category would include:
    - Food and Nutrition Services
    - Environmental Services
    - Plant Operations
    - Central Sterile Supply
    - Volunteer Services
    - Materials Management
    - Supply Chain
    - Laundry and Linen
    - Administrative Assistants
- Moderate Risk: Positions that have occasional or indirect contact with covered information. System access does not allow information or data to be altered. Examples of positions/areas in this category include:
    - Marketing
    - Security Services
    - Accreditation
    - Legal/general counsel
    - Direct patient care positions
    - HIM staff
    - Billing staff
    - Leadership positions (excluding Executive Leadership Team)
- High-Risk: Positions that have recurring direct access to or the ability to access or alter covered information without supervision or other confidential information. Examples of positions/areas in this category include:
    - Non-information technology personnel who have privileged user access (e.g., system, application, database administrators)
    - Finance
    - People & Culture (HR)
    - Information and Technology Services
    - Information security
    - Audit and Compliance
    - Providers (mid-level and higher)
    - Pharmacists
    - Executive Leadership Team (ELT)

Position categorization levels will be reviewed and revised by the CISO and People and Culture on an annual basis.

Position reviews will include all the same requirements as a pre-employment background investigation. If the results of a position review produce adverse information about the individual, his/her access to

covered information will be immediately removed until a time at which the organization has determined what action (e.g., position reassignment, suspension, termination, etc.) will be taken.

Documentation Retention:
Records related to background investigations will be retained in accordance with federal and state requirements. If a lack of guidance exists, documentation will be retained for a period of time no less than 6 years from the date of the documentation.

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management policy

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.