CONE HEALTH	**Guideline:** ITS Application Security Development 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, Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI) and sensitive and confidential data (i.e., covered information) it creates, receives, maintains, and/or transmits. The purpose of this document is to define Cone Health's information security policies. Procedures, guidelines, standards and processes are defined under separate documentation that can be referenced using links within the policy/procedure documents.

Scope and Goals:
The scope of this procedure is to identify and define the following requirements throughout the various stages of application development:

- Security related processes and requirements - Discovery phase.
- Security checks, test plans, and profile requirements - Design phase.
- Secure coding practices - Coding phase.
- Quality assurance and secure code review - Testing stage.
- Security requirements review - Deployment stage.
- Ongoing application security support and maintenance - Post-deployment stage.

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

- Revisions, implementation, workforce education, interpretation, updates, and enforcement of this procedure.
- Manage or oversee the management of the application security development program.
- Ensure an independent pre-production review and testing of security controls for all new applications, an independent pre-production review and testing of security controls for all new applications.
- Identification of industry accepted secure coding practices that will be utilized when developing new applications.
- Ensure that production environments are not being used for development and testing purposes and that they do not contain and in-development code.

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

- Implementing the requirements outlined in this procedure for all applications that process, store, and/or transmit covered information.

- Maintaining security of their applications by actively supporting them pre/post deployment.

Secure Application Development Stages:
The following procedure provides details surrounding the unique requirements for developing secure applications that will be used in the production environment.

STAGE 1 - Requirements (Discovery):
During this phase, the development team will:

- Perform threat modeling/risk assessment to determine what potential security threats the new application will be exposed to once in production, as well as the operation environment.
- Determine the sensitivity (i.e., classification) level of the application, based on the data that will be processed, stored, and/or transmitted by the new application.
- Identify and document what security requirements, such as ports, protocols, and intended services (i.e., Secure Configuration Management procedure), are required to be built into the new application. Depending on the data sensitivity, application functionality, and potential threat(s) the new application will be exposed to, additional security features beyond what is required at a minimum by policy, must be required to be built into the new application.

STAGE 2 – Design:
During this phase, the development team will:

- Identify mandatory security controls that need to be built into the application.
- Identify which secure coding guidelines (i.e., OWASP, Android Secure Coding Standard, CERT C++ Coding Standard, SEI CERT Perl Coding Standard, SEI CERT Oracle Coding Standard for Java, etc.) will be utilized by the development team.
- Identify how and by whom (i.e., internal vs. third party) the application source code will be tested for security, functionality, performance, etc.

STAGE 3 – Development (Coding):
During this phase, the development team will:

- Ensure that only project team members are allowed read-write access to the source code system. Access to project artifacts and source control systems will always be strictly controlled throughout all phases of application development.
- Managers responsible for applications perform and document periodic code reviews to ensure that security controls are implemented correctly.
- Follow the secure coding practice identified in the previous phase.
- Document all activities required by the project plan.
- Periodically perform quality review exercises.
- Remove backdoors, debugging tools, unnecessary scripts/lines of code, etc.
- Avoid using “hidden commands” in the application grammars to circumvent authorization and authentication paths.

STAGE 4 – Testing:
During this phase, the development team will:

- Ensure all application testing is performed in a test/development environment and never in production.
- Ensure that all production security requirements are followed if "live" covered information will be used in the test/development environment.
- Ensure testing includes all previously identified security requirements, usability, and effects on other systems.
- Ensure code reviews (manual or automated) are conducted by someone other than the code author. Note: Third-party code reviews will be performed whenever possible and at the discretion of the CISO.
- Ensure code review only occurs after all final changes have been made and developer access has been restricted to ensure no changes are made during the testing phase.

NOTE: All remediation activities associated with code review and security testing will be completed in the test phase.

STAGE 5 – Deployment:

During this phase:

- The CISO will review the outcomes from the test phase to ensure that security requirements have been adequately addressed. The CISO will provide formal approval that the application is ready for production. Without this approval, the application will not be moved into the production environment.
- The deployment team will create a fallback plan in the event that a deployment runs into unforeseen issues or causes problems in the production environment.
- Deployment of the new application into the production environment will be approved by the Change Advisory Board (i.e., change control process). Refer to the Change Management Procedure.

STAGE 6 – Post-Deployment:

- The CISO and the application owner will perform a review within the first week of the application becoming operational, to ensure that security controls are functioning as required. Security reviews going forward will fall under the organization's vulnerability management program.
- If source code was developed by a third party, a copy of the code will be put in escrow.
- Any application code changes from this point on will be put through the same process as the initial code.

Documentation Retention:

Documentation will be retained for a period of no less than 6 years from the date of the deployment.

Exception Management:

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

Guideline: ITS Application Security Development 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.