Procedure: Secure Software Development

Purpose
The purpose of this procedure is to ensure that information security requirements are established across the lifecycle of in-house developed information systems, which includes testing, implementation and updates of information systems.

General
The following general rules shall apply:

- Applications created or deployed inside the ESD IT environment must follow a standardized application lifecycle established by management.
- Applications should be actively maintained and require periodic updates to address vulnerabilities. If an application is no longer supported by the vendor, developer, or another party, it must be evaluated for replacement.
- Development, testing, and operational environments must be separated.
- Configuration changes to the system must be approved by the Designated Information Security Officer prior to the change being implemented.
- The production data source must be sanitized before use in development or test environment and production/test access controls must comply with production standards.
- Test data and accounts must be removed before a production system becomes active.
- Code must be approved prior to deploying to production. The approver must not be the author of the code but be someone who can understand the actions of the code, such as a software development manager or a peer developer.

Software Development
When developing software, the following rules shall apply:

- All software development personnel must receive annual applicable training in writing secure code for their development frameworks and environment.
- Access to program source code should be restricted based on principle of least privilege.
- For applications that store or transmit confidential information, security controls must be implemented to limit output to minimum necessary as defined by the user.
- Any outsourced software development should comply with the Secure Software Development Lifecycle Standard
- Modifications to externally developed software packages must be limited to necessary changes and all changes should be strictly controlled.
- All newly developed software and updates or revisions to existing software must be fully tested and accepted prior to deployment to the production environment.

System Acceptance
Acceptance criteria must be provided by the application/resource owner and should specify:

- operational and functional requirements of the application,
- performance and capacity requirements,
- data classification,
- hardware specifications, if applicable.

All acceptance criteria must be satisfied before any system or application can move into a production environment.

Timeline for Implementation of Procedure
Given the required changes to ESD processes to fully implement this procedure, new technology systems will be subject to this procedure immediately while existing processes or systems will be reviewed as required by the procedure's periodic review. If an operating practice is needed from IT as part of the procedure, IT will develop and have implemented that process before running proposed technology system through it. Procedure to be fully implemented by September 1, 2024.