

9400-P180: Information Security in the System Lifecycle

I. PURPOSE

To ensure that information security is addressed during the entire lifecycle of an information system to control the costs and maximize the effectiveness of security controls.

II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agencies”).

III. POLICY

- A. Security of information and information technology (IT) resources shall be a consideration during the entire life cycle of all State-purchased or developed systems and applications.
- B. There shall be a structured process for the adequate planning and design of security for new systems or systems undergoing a major upgrade. Whether or not the State chooses to build or purchase the system, its lifecycle includes phases such as those in the table below.

Phase Description	Build Consideration	Buy Consideration
Requirements & Analysis	✓	✓
Design & Engineering	✓	Product selection
Development	✓	✓
Testing & Deployment	✓	✓
Operations & Maintenance	✓	✓
End-of -Life	✓	✓

- C. Requirements and Analysis. Information security activities shall be present in the requirements and analysis phase and include:
 - 1. Data Stewards and/or information technology resource owners shall include security requirements and/or capabilities as part of the system specifications for new systems or modifications to existing systems/applications.
 - 2. The security requirements shall be based on policy, legislation, contract, or generally accepted industry best practices.
 - 3. The security requirements shall be documented by the Data Stewards.
 - 4. The security requirements shall reflect the results of a risk assessment in terms of risks to the confidentiality, integrity, and availability of the system and its information, risks to the State’s technical infrastructure and the risk to the State or State agencies should the controls that implement the requirements fail (threat impact).

9400-P180: Information Security in the System Lifecycle

5. The Data Steward or their designee (e.g., project manager, etc.) shall have review and security signoff/acceptance responsibilities before the development can advance to the next phase.
- D. Design and Engineering. Information security activities shall be present in the design and engineering phase and include:
1. Functional security requirements shall be refined into specific technical and non-technical security controls to be included in the system's technical design or purchase specifications.
 2. Security planning shall be part of the development process for all new business application systems.
 3. If the technology and/or operational environment cannot provide or support the required controls, other types of controls shall be used to achieve the desired level of protection or a request for an exception shall be made per Policy 10100-P110: Security Policies, Standards, & Procedures.
 4. For purchased systems, confirm that the required security controls are present when the product is in its final operational configuration.
 5. Outsourced development activities shall be structured and monitored to ensure that the security controls used during development, testing, and deployment are equal to or more stringent than the security requirements of the activity counterpart in the State/agency environment.
 6. To the extent possible, development/engineering environments shall be separate from the production environments.
 7. If live (real) data is used in the development/engineering or test environment, it shall be protected in the same manner as in the production environment.
 8. Security controls shall be in place and operational before systems are placed into a production environment.
- E. Testing and Deployment. Information security activities shall be present in the testing and deployment phase and include:
1. To the extent possible, a separate test environment shall be used to prevent the possibility of test or development-induced impact on the production environment or processes.
 2. To the extent possible, test data shall not contain any confidential information. If it must be used, it shall be protected in the same manner as in the production environment.
 3. Test plans shall be created to verify the presence and effectiveness of the security controls. The results of security testing shall be documented and used as input for acceptance of risk determination.

9400-P180: Information Security in the System Lifecycle

4. Only the Data Steward or designee (e.g., project manager, developer, or other authorized individual working on the Data Steward's behalf) shall have the authority to promote software from the development/test environment to the production environment. To the extent possible, individuals authorized to promote software should not be the developer or the tester.
 5. Users shall be appropriately trained on their security (and operational) responsibilities for the new system before they are allowed to access the system.
 6. Systems shall not be placed into the environment (e.g., on the network) without the formal approval (acceptance of risk) of the Data Steward. Systems that have the potential to place two or more agencies at risk shall be placed into operation only with the concurrence and coordination of the Data Stewards and the Office of the Chief Information Officer (OCIO).
- F. Operations and Maintenance. Information security activities shall be present in the operations and maintenance phase and include:
1. Access to source code libraries and production executables shall be strictly controlled such that only specific personnel with a duty requirement to do so have access.
 2. Restrictions shall be placed on installing software (see Policy 3100-P160: Communications and Operations Management).
 3. Agencies shall administer an agency-developed change management process requiring management approval for all changes made to production application systems (see Policy 3100-P160: Communications and Operations Management).
 4. Patch management (vulnerability management) shall be a part of the operations and maintenance phase of the system lifecycle. Security-relevant vulnerabilities, recommended patches, and implementations of upgrades shall be monitored and managed (see Policy 9400-P183: Technical Vulnerability Management).
- G. End-of-life. Information security activities shall be present in the end-of-life phase and include:
1. All IT resources that belong to the State shall be thoroughly purged of all information before any form of non-volatile media leaves the State's control (e.g., goes to salvage, redistribution, etc.) (see Policy 9400-P164: Preparation of Electronic Devices and Media for Disposal).