APPLICATION SECURITY GUIDELINES IN THE SDM

Purpose: The purpose of these guidelines is to ensure that security is built into the application from project concept through implementation for all applications administered by the Department of Information Technology (DoIT).

Guidelines: The guidelines listed below shall be used to consider security requirements during the planning, design, and implementation of new or enhanced applications. Applications require different levels of security; therefore all the activities below may not be necessary for any given application. The documentation requirement of each phase, however, is required for all projects.

Project Concept Phase

During the project concept phase, a risk assessment shall be made of the proposed application to determine the appropriate level of security needed to meet the business requirements of the system. The specific project needs, including security, shall be documented and approved by the agency

DoIT, in cooperation with the agency, shall evaluate the business purpose of the system for the following concerns:

a) Identify legal and policy requirements
b) Identify potential losses arising from accidental or unauthorized activities, poor decisions based on unreliable information, or business costs due to system unavailability
c) Identify potential adverse customer reactions arising from system unavailability or unreliable information
d) Document the issues identified

Project Design Phase

During the project design phase, the business needs for security must be integrated into the system design. The project's technology and processes for using the system should be examined for their ability to support the confidentiality, integrity, authorization and availability objectives identified in the Project Concept Phase. The security considerations and recommended control measures shall be documented in the project specifications and be approved by the agency.

DoIT shall conduct an analysis of the functional and design specifications to address the following concerns:

a) Ensure individual accountability for all transaction actions
b) Ensure incoming data are complete, accurate, and authorized before completing the transaction
c) Assign program function and data access privileges to users on a need-to-know basis and segregation of duties principle
d) Identify critical operations or confidential data that require special handling
e) Ensure auditability of transactions from origination to destination
f) Ensure audit trails meet the business and/or regulatory requirements
g) Establish data retention/destruction requirements and provide backup and recovery procedures to satisfy business continuity requirements
h) Document security design and specifications

APPLICATION SECURITY GUIDELINES IN THE SDM

In addition, DoIT shall analyze the operating environment including networking, server configuration, programming languages, physical security, and administrative processes to address the following concerns:

a) Review the adequacy of the physical and environmental controls for protecting the servers and infrastructure
b) Ensure sufficient authentication and access control mechanisms are in place to allow only authorized access to system resources
c) Identify risks arising from transmissions of clear-text data and passwords as well as the need for encryption methods
d) Identify privileged functions that require special handling
e) Identify privileged administrative duties that require special treatment
f) Ensure proper change control procedures are in place for promoting application changes into production
g) Document analysis

Implementation and Acceptance Phase

During the implementation and acceptance phase, the test plan and testing results are reviewed for assurance that the security measures satisfy the business requirements of the functional specifications

DoIT, in cooperation with the agency, shall review all security implementations to verify that

a) The risk analysis was documented in the project concept phase
b) The security considerations and recommended control measures were documented in the functional/design phase
c) The system testing covers all recommended control measures specified in the functional and design documentation
d) That the testing effort is appropriate to fully test the security of the application
e) Document that the completed application complies with all business requirements

Accountability: These guidelines apply to all applications created and or administered by the Department of Information Technology. It is the responsibility of each DoIT Division Director and Bureau Chief or their designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: These guidelines provide a common approach to the security of an application and apply to all applications administered by the DoIT.

Reference: System Development Methodology (SDM)
Application Security Procedure
Application Security Scan Request Form
Security Guidelines in the SDM
IT Standards Exception Policy
Payment Card Industry Data Security Standards Application Development and Maintenance Procedures
Payment Card Industry Data Security Standards Application Development and Maintenance Form