

State of Vermont

Minimum Security Standards for Application Development Policy



Date: 11-02-10
Approved by: Tom Pelham
Policy Number:

Contents

1.0 Introduction 3

 1.1 Authority 3

 1.2 Purpose 3

 1.3 Scope 4

2.0 Policy 4

 2.1 General 4

 2.1.1 Concept Phase 4

 2.1.2 Project Design Phase 5

 2.1.3 Implementation and Acceptance Phase 6

 2.2 Application Security Review Guidelines 6

3.0 Policy Notification 7

1.0 Introduction

Application security encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application.

Applications only control the use of resources granted to them, and not *which* resources are granted to them. They, in turn, determine the use of these resources by users of the application through application security.

1.1 Authority

The State of Vermont is authorized to undertake the development of enterprise architecture policies and standards. The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), "to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government."

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

Security testing techniques search for vulnerabilities or security holes in applications. These vulnerabilities leave applications open to exploitation. Ideally, security testing is implemented throughout the entire software development life cycle (SDLC) so that vulnerabilities may be addressed in a timely and thorough manner. Unfortunately, testing is often conducted as an afterthought at the end of the development cycle, or not at all.

The purpose of this policy is to ensure that security is built into the application from project concept through implementation for all applications administered or used by the State of Vermont.

1.3 Scope

This policy applies to all software applications that are being developed by or for State of Vermont staff and/or consumers of State services, regardless where the infrastructure and/or data reside.

2.0 Policy

The development phases 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, whether developed in house or by contractors. All contracts written to procure development services shall include statements that require risk assessment and penetration testing as appropriate.

2.1 General

Security is an important part of the system life cycle process. Systems developed or acquired must have documented security specifications. It is very difficult to produce secure applications consistently without some structure in place to do so.

To keep risk to an acceptable level agencies and departments shall ensure that the proper security controls will be implemented for each application. These controls will vary in accordance with the sensitivity and criticality of each application. Minimum standards that should be applied to the development and administration of applications are greatly influenced by the relative sensitivity of the data and information flowing through the application.

Application level security must be planned from the start of any project and should be reviewed during any upgrade, enhancement or major maintenance activity to existing projects. Security planning should include an analysis of security requirements, which may include the following topics:

1. Review of current and future business and security goals of the system.
2. Analysis of system assets relative to the value and sensitivity of the data.
3. Analysis of potential risks to the assets.
4. Review of regulatory requirements regarding both security and privacy of data.
5. Analysis of both internal and external threats to security.

2.1.1 Concept Phase

During the project concept phase, a written risk assessment shall be started (by the appropriate business unit data owner and IT application developer) 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 project team, in cooperation with the agency throughout the development cycle.

The business purpose of the system shall be evaluated for, but not limited to, 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

As part of the analysis of risk, the project team should consider:

- a) Fraud
- b) Theft
- c) Destruction
- d) Breach of privacy
- e) Denial of service

2.1.2 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.

The Application Developer and the agency IT manager 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 the ability to audit 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

For mission critical or Enterprise applications additional reviews by state/Agency security directors or others may be required.

The final goals of the security system should include:

1. Confidentiality of the data
2. Authentication of the data
3. Integrity of the data
4. Non-repudiation of the data
5. Availability of the data
6. Auditing of the data

2.1.3 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

The Application Developer in cooperation with the agency/department IT staff, 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

2.2 Application Security Review Guidelines

The Application Developer and the IT manager 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

3.0 Policy Notification

Each state agency is responsible for ensuring that employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.