HPOL#07
Acquisition, Development, and Maintenance of Software

(Version 1.0)

Table of Contents

7.1. SCOPE AND OBJECTIVES 2
7.2. POLICY STATEMENT 3
7.2.1. SECURITY REQUIREMENTS OF THE SYSTEM 3
7.2.1.1. Security Requirements Analysis and Specification 3
7.2.2. SECURITY IN APPLICATION SYSTEM 3
7.2.2.1. Application System 3
7.2.2.2. Policy on the use of Cryptographic Controls 4
7.2.2.3. Encryption 4
7.2.2.4. Digital Signatures 4
7.2.2.5. Non Repudiation Services 5
7.2.2.6. Key Management 5
7.2.3. SECURITY OF SYSTEM FILES 5
7.2.3.1. Control of Operational Software 5
7.2.3.2. System Test Data 6
7.2.3.3. Access Control to Program Source Library 6
7.2.4. SOFTWARE ACQUISITION 6
7.2.4.1. Acquisition Planning 6
7.2.4.2. Contracting 7
7.2.5. SECURITY IN DEVELOPMENT AND SUPPORT PROCESS 8
7.2.5.1. Change Control Process 8
7.2.5.2. Technical Review of Operating System Changes 8
7.2.5.3. Restrictions on Changes to Software Packages 9
7.2.5.4. Covert Channels and Trojan Code 9
7.2.5.5. Outsourced Software Development 10
7.2.5.6. Development of Maintenance Plan 11
7.2.6. PROJECT MANAGEMENT 11
7.2.6.1. Use of Project Management Methodology 11
7.2.6.2. Information Security as a Component of Project Management 11

7.1. SCOPE AND OBJECTIVES

In order to maintain a high level of information security, the security requirements of an information system should be considered, documented and planned for, prior to the development or acquisition of the system itself.

Government organizations should define and implement the procedures for acquisition, design and development as well as maintenance of software in a standardized manner. These procedures and methods should delineate the various aspects of specifications, configuration, development and procurement cycle of the software while ensuring that they are of required quality with appropriate controls installed in them and that they meet the desired business objectives.

This policy establishes guidelines for building security into information systems including infrastructure, business applications and user-developed applications, and to maintain security of application systems and information processing facilities.

7.2. POLICY STATEMENT

7.2.1. Security Requirements of the System

7.2.1.1. Security Requirements Analysis and Specification

7.2.1.1.1. All statements of business requirements for new information systems or enhancements to existing information systems must specify control and system security requirements.

Explanatory Notes

It is the responsibility of the business process owner who develops the statements of business requirements to identify and include control and security requirements.

7.2.1.1.2. Systems security requirements must reflect the business value of the information assets involved.

Explanatory Notes

Systems security requirements must be in accordance with the Asset Classification Policy and associated procedures, and the potential damage that may be caused due to absence of sufficient security.

7.2.2. Security in Application System

7.2.2.1. Application System

7.2.2.1.1. Business process owners must ensure that adequate application controls are in place in the applications.

7.2.2.1.2. Applications developed within the government organization must be developed in accordance with an accepted systems development and maintenance methodology, and as per the security requirements reflecting business needs.

7.2.2.1.3. Appropriate controls including audit trails and activity logs must be designed into application systems.

Explanatory Notes

Appropriate controls should include but not be limited to validation of input data, internal processing and output data.

7.2.2.2. Policy on the use of Cryptographic Controls

7.2.2.2.1. Cryptographic controls must be implemented in accordance with the government organization's standards and procedures for encryption.

Explanatory Notes

An assessment must be carried out to identify the needs, methodology, business areas and usage of cryptographic controls, which may include key management, roles and responsibilities, level of cryptography, standards to be adopted, methodology to recover information lost due to improper handling of controls, and implementation of policy.

7.2.2.2.2. The usage of cryptographic controls must comply with applicable laws and regulations.

7.2.2.3. Encryption

7.2.2.3.1. The government organization must have a defined type of encryption algorithm used and length of cryptographic keys, as per the criticality of the business processes.

7.2.2.3.2. The length of the cryptographic keys must comply with applicable cyber laws and regulations.

7.2.2.4. Digital Signatures

7.2.2.4.1. A legal framework must be developed and enforced for the usage of digital signatures and must comply with applicable cyber laws and regulations.

7.2.2.5. Non Repudiation Services

7.2.2.5.1. Non repudiation services shall be used to resolve disputes about occurrence or non–occurrence of an event or action.

7.2.2.6. Key Management

7.2.2.6.1. The government organization must identify the secret key techniques and public key techniques to be used, as per the requirements.

7.2.2.6.2. All secret, public and private keys must be protected against modification, destruction and unauthorized disclosure.

7.2.2.6.3. The government organization must have formal standards, procedures and methodology for key management.

Explanatory Notes

Standards, procedures and methodology for key management should include but not be limited to generation, distribution, destruction, storage, recovery, revocation, archiving, and obtaining of public key certificates.

7.2.3. Security of System Files

7.2.3.1. Control of Operational Software

7.2.3.1.1. All changes to software in the Production environment should only be made by authorized personnel and should be in accordance with the government organization’s Change Management Procedures.

7.2.3.1.2. Software source code must be stored in a physically separated place from the production environment.

7.2.3.1.3. All attempts to access operational software must be logged. The government organization must review the logs at pre-determined intervals.

7.2.3.2. System Test Data

7.2.3.2.1. Where copies of operational data are used for testing purposes, they must be appropriately de-personalized.

7.2.3.2.2. System test data must be subject to the same level of access controls as the production data from which it was derived or extracted.

7.2.3.2.3. Access to system test data must be logged and monitored on a periodic basis.

7.2.3.3. Access Control to Program Source Library

7.2.3.3.1. Access to source code libraries must be restricted in accordance with the government organization’s Change Management Procedures.

7.2.3.3.2. Modified source code should be deposited into the library as a new version of the source code. Overwriting or modification of existing source code in the library is expressly prohibited.

7.2.3.3.3. Only the designated and authorized source code librarian (or equivalent) should have ‘write’ access to the source code library.

7.2.3.3.4. Issue and return of code must be in accordance with the government organization’s procedures for this purpose.

7.2.4. SOFTWARE ACQUISITION

7.2.4.1. Acquisition Planning

7.2.4.1.1. The government organization’s strategy, initiating the planning process, and establishing general practices for planning of the software acquisition, requires to be instituted.

Explanatory Notes

The objectives behind acquiring the software should be identified, critically reviewed and finalized. The final objectives should then be translated into a procurement strategy that would essentially involve deciding on the type of the software to be acquired, e.g., commercial on-the-shelf, modified on-the-shelf, or fully customized application.

7.2.4.1.2. The functionality that the software should address, is to be defined, analyzed and frozen.

Explanatory Notes

This would also involve minimum, but critical functional specifications that a new system must address and provide for, and the yardsticks for specific software quality. These requirements should be included in the Bidding Document.

7.2.4.2. Contracting

7.2.4.2.1. Prospective vendors should be identified.

Explanatory Notes

Prospective vendors who would provide documentation of the software, demonstrate the functionality and offer formal proposals should be identified. The supplier data along with credentials and past performance should also be reviewed.

7.2.4.2.2. Contract requirements should be prepared.

Explanatory Notes

Contract requirements detailing expected quality, acceptable performance and criteria, contract provisions, payments options and their direct linkage to deliverables should be prepared.

7.2.4.2.3. Once the proposals are received, they should be evaluated.

Explanatory Notes

The proposals are evaluated against the desired and critical functionality, quality specifications, payment terms, future maintenance service, and support from vendors. Based on the results of the evaluation, the supplier should be selected by management of the government organization.

7.2.5. SECURITY IN DEVELOPMENT AND SUPPORT PROCESS

7.2.5.1. Change Control Process

7.2.5.1.1. The government organization's Change Control Procedures must be compliant with or based on an accepted system development and maintenance methodology.

Explanatory Notes

The change control processes must be used for all changes (including configuration changes) to software, hardware, and communications links.

7.2.5.1.2. System documentation must be updated to reflect changes.

7.2.5.1.3. An audit trail and version control must be maintained for all changes made.

7.2.5.2. Technical Review of Operating System Changes

7.2.5.2.1. Government organization Change Control Procedures must address all changes, enhancements, installation of new software patches and version updates.

7.2.5.2.2. Prior to application of the updates in the production ('live') environment, the government organization must test the operation and compatibility of existing applications with the proposed updates.

7.2.5.2.3. All updates, patches, version changes, etc., must be tested and reviewed for security controls prior to implementation.

7.2.5.3. Restrictions on Changes to Software Packages

7.2.5.3.1. Modifications to software packages should be discouraged.

Explanatory Notes

As far as possible, and practicable, vendor-supplied software packages should be used without modification.

7.2.5.3.2. All modifications (including configuration changes, changes to reports, etc.) to software packages must be made in accordance with the government organization's Change Control Procedures.

Explanatory Notes

Modifications to software packages would include but not be limited to configuration changes, changes to reports, etc.

7.2.5.4. Covert Channels and Trojan Code

7.2.5.4.1. All software and hardware must be acquired from trusted sources.

Explanatory Notes

Covert channels and Trojan code could lead to malfunctioning of the system, and also compromise the system's confidentiality, integrity and availability.

To protect the system from being compromised, the government organization's Change Control Procedures must include procedures for the inspection of software source code for possible 'Trojan' code or 'Covert' channels.

7.2.5.4.2. The government organization must require that the vendor guarantees that the software is free of 'Covert channels' and 'Trojan' code when purchasing the software from third parties.

7.2.5.5. Outsourced Software Development

7.2.5.5.1. A process must be implemented to verify the vendor's compliance with the government organization's requirements.

7.2.5.5.2. All outsourced developments must adhere to the "Compliance Measurement" Policy of the government organization.

Explanatory Notes

The elements of compliance will include but not be limited to licensing arrangements, code ownership, intellectual property rights, and third party agreements.

The government organization's requirements for outsourced software development must include compliance with the organization's Change Control Procedures.

The government organization's requirements for outsourced software development must include compliance with an acceptable systems development and maintenance methodology.

7.2.5.5.3. If third party software is being considered for critical business activity, the government organization must procure the source code from the third party.

7.2.5.5.4. Where the source code is not procured, the third party must provide the source code to an outside party who will hold the source code in escrow each time the source code is revised.

7.2.5.5.5. All documentation must be reviewed by the government organization prior to being released to third parties.

Explanatory Notes

Documentation which describes systems or systems procedures, must be reviewed by the government organization to ensure that confidential information is not being inadvertently disclosed.

7.2.5.6. Development of Maintenance Plan

7.2.5.6.1. The maintenance process should be developed by the government organization.

Explanatory Notes

The maintenance process should be based on existing resources and future expectations. The approach is dependent upon the maintenance tools and different methods adopted for maintenance.

The plan should clearly state the critical personnel required for maintenance efforts. The requirement should be compared with availability of skilled personnel, a gap analysis should be performed and the manpower resource plan crystallized. The maintenance staff should be deployed taking into account core competence, training, experience and availability.

The plan should include resources such as systems, software, hardware, and other ICT infrastructure components which are to be used for maintenance.

The plan should provide for methods of monitoring the performance of the maintenance work performed in terms of issues handled, the lead time for solutions and performance measurement.

7.2.6. PROJECT MANAGEMENT

7.2.6.1. Use of Project Management Methodology

7.2.6.1.1. The government organization requires that all information security projects must be managed in accordance with the organization’s accepted Project Management Methodology.

7.2.6.2. Information Security as a Component of Project Management

7.2.6.2.1. The government organization requires that Information Security must be considered as a component of all projects undertaken by or on behalf of the organization.

Explanatory Notes

All projects must contain plans to manage information security relevant to the project and such plans must be in accordance with the government organization’s associated Information Security Policies.