Information Technology Branch
Information Technology Systems Acquisition, Development and Maintenance Technical Standard

Information Management, Administrative Directive A1461

Cyber Security Technical Standard #6

November 20, 2014

Approved: **Date**: November 20, 2014

1. Purpose

This technical standard establishes requirements and controls for managing the lifecycle of information technology systems ensuring that security requirements are identified early on as part of the business needs, and ensures that information technology acquisition takes into account information protection.

2. Scope

This technical standard is intended to apply to people, equipment, application systems and processes that fall within the direct organizational control and support responsibilities of the Information Technology Branch of Corporate Services Department.

3. Exceptions and Compensating Controls

In cases where business requirements or technology limitations prevent direct compliance with an implementation expectation, compensating controls can be proposed that meet the statement objective. If an interpretation is required, contact the Program Manager, IT Security and Risk Assurance Program, Information Technology Branch for guidance. Special cases where exceptions are required to meet business requirements or technology limitations need to be documented and approved.

4. Standards and Implementation Expectations

Implementation expectations establish baseline behaviors and actions that are consistent with industry standards or best practices to meet the technical standard statements. It is the intention of this section to establish baseline security requirements in support of business operations, not to impede business operations or define specific technologies or methodologies.

The technical standards do not provide exacting and prescriptive guidance on exactly how to perform everything stated within the standard. In most cases, additional specific how-to procedures will need to be developed.

4.1. Security Requirements of Information Technology Systems Technical Standard

4.1.1. Security controls must be identified as part of the business requirements for new information technology systems or major enhancements to existing information technology systems.

4.1.1.1. Implementation Expectations

When required a security threat and risk assessment should be completed during the requirements phase when developing, implementing major changes to, or acquiring information technology, to:

- Identify the security requirements necessary to protect information technology systems; and,
- Assign a security classification to the information and information

technology systems.

The risk assessment should also identify the following information:

- Roles and responsibilities for information technology system security management;
- Any specific procedures used to mitigate risks and protect the information technology system;
- Monitoring procedures; and,
- Communication procedures for security-relevant events and incidents.

At implementation, the IT Branch should ensure that sufficient controls are in place to mitigate the risk of information loss, error or misuse from information technology systems.

4.2. Security of System Files Technical Standard

4.2.1. The implementation of software on production information technology systems must be controlled.

4.2.1.1. Implementation Expectations

The IT Branch should implement procedures to control software installation on production information technology systems to ensure that:

- Updates of production information technology systems are planned, approved, impacts assessed, tested, logged and have a rollback plan;
- New releases of software are reviewed to determine if the release will introduce new security vulnerabilities;
- Modifications to production software are logged;
- The number of employees able to perform the updates is restricted and kept to a minimum; and
- Vendor supplied software is maintained at the supported level.

4.2.2. Test data must be protected and controlled using the same procedures as for data from production information technology systems.

4.2.2.1. Implementation Expectations

The IT Branch should implement procedures to ensure that:

- Sensitive or personal data from production information technology systems is not used as test data;
- Using test data extracted from production information technology systems should be authorized and logged to provide an audit trail;
- Test data is protected with controls appropriate to the security classification of the information and information technology systems; and,
- Data from production information technology systems is removed from the test environment once testing is complete.

4.3. Security in Development and Support Processes Technical Standard

4.3.1. Changes to software must be controlled by the use of formal change control procedures.

4.3.1.1. Implementation Expectations

A change control process should be implemented for new information technology systems which can include:

- Requiring that change requests originate from authorized personnel;
- Requiring that proposed changes are reviewed and assessed for impact; and,
- Logging all requests for change.

A change control process should be implemented for production information technology systems which can include:

- Requiring that change requests originate from authorized personnel;
- Documenting back out plans;
- Documenting approval of changes proposed prior to the commencement of the work;
- Documenting the acceptance tests and approval of the results of acceptance testing;
- Updating operations and user documentation with the details of changes;
- Maintaining version control for changes to the software; and,
- Logging all requests for change.

4.3.2. Information technology systems must be reviewed and tested when operating system changes occur.

4.3.2.1. Implementation Expectations

Processes should be in place to provide appropriate notification to affected parties of production system changes to allow for:

- Sufficient time for the review and testing of information technology systems prior to implementation;
- Ensure dependent information technology systems will not be compromised by the change; and,
- Information technology testing with the changes to the production system in a separate (i.e. test) environment.

4.3.3. Controls must be applied to secure outsourced information technology development.

4.3.3.1. Implementation Expectations

The IT Branch should consider the following when outsourcing information technology development:

- Procurement guidance for licensing, ownership and intellectual property rights;

- Rights of access for audit and certification of the quality and accuracy of the work; and,
- Contractual requirements for quality and security functionality of the information technology systems.

4.4. Technical Vulnerability Management Technical Standard

4.4.1. Regular assessments must be conducted to evaluate information technology vulnerabilities and the management of associated risks.

4.4.1.1. Implementation Expectations

Vulnerabilities which impact information technology systems should be addressed in a timely manner to mitigate or minimize the impact on operations. Processes should be established that identify, assess and respond to vulnerabilities which may impact information technology systems by:

- Regularly assessing information technology systems for known vulnerabilities;
- Monitoring external sources of information on published vulnerabilities and assessing the risk of such;
- Testing and evaluating options to mitigate or minimize the impact of vulnerabilities; and
- Applying corrective measures to address the vulnerabilities.

5. Reference

Further information can be found in:

ISO 27002, Chapter 12 – Information Systems Acquisition, Development and Maintenance