Information Technology Branch Cyber Security Incident Management Technical Standard

Information Management, Administrative Directive A1461

Cyber Security Technical Standard # 7

November 20, 2014

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

1. Purpose

This technical standard identifies the requirement to ensure that Information Technology Branch cyber security incident management processes are established. The process will enable the Information Technology Branch to identify, assess, manage, mitigate and accurately communicate facts of cyber security incidents.

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. Technical 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. Reporting Cyber Security Events and Weaknesses Technical Standard

4.1.1. Cyber security events must be reported through appropriate channels as quickly as possible.

4.1.1.1. Implementation Expectations

The IT Security and Risk Assurance Program should develop and maintain a City-wide standard for reporting cyber security events.

This standard should:

- Ensure Employees can report observed or suspected threats or events by telephone, electronic form or e-mail;
- Report cyber security incidents which result in real or perceived

breaches of privacy to the Departmental FOIP Coordinator; and,
- Report cyber security incidents to the IT Security and Risk Assurance Program, Information Technology Branch.

4.2. Management of Cyber Security Incidents and Improvements Technical Standard

4.2.1. Incident management responsibilities and procedures must be established for the IT Branch to ensure a quick, effective and orderly response to cyber security incidents.

4.2.1.1. Implementation Expectations

The IT Security and Risk Assurance Program should establish a process for reporting, managing, responding to and recovering from cyber security incidents.

Security incident management processes for continuous improvement should be established and includes:
- Monitoring incidents using statistical analysis of frequency, types and locations of security incidents;
- Analyzing incidents and responses;
- Determining requirements for awareness and training;
- Improving the security of information technology applications and infrastructure through monitoring and the reporting of security events; and,
- Integrating automated alarms and other security incident detection technology with logs and auditing systems.

4.2.2. The types, volumes and costs of cyber security incidents must be quantified and monitored.

4.2.2.1. Implementation Expectations

The IT Security and Risk Assurance Program is responsible for monitoring and evaluating cyber security incidents by:
- Using statistical analysis of incident frequency, type and location to identify trends;
- Ensuring incident reports and trends are used to promote continuous improvement of IT Branch processes, security awareness and training programs, and IT Branch business continuity and disaster recovery plans; and,
- Evaluating the effectiveness of incident management, response and reporting.

5. Reference

Further information can be found in:
- ISO 27002, Chapter 13 – Information Security Incident Management