Information Technology Branch Organization of Cyber Security Technical Standard

Information Management, Administrative Directive A1461

Cyber Security Technical Standard # 1

November 20, 2014

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

1. Purpose

This technical standard identifies the requirements to ensure that organizational roles and responsibilities for cyber security management are identified, implemented and managed following a set of baseline security requirements.

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. Internal Parties Technical Standard

4.1.1. The Corporate Services Department will support cyber security through clear direction, demonstrated commitment, explicit assignment and acknowledgement of cyber security responsibilities.

4.1.1.1. Implementation Expectations

In order to facilitate the development of a security program a number of groups or individuals have been identified with distinct security roles. These groups and the identified roles are:

- General Manager, Corporate Services
- Branch Manager, Information Technology Branch, Corporate Services
- Program Manager, IT Security and Risk Assurance, Information Technology Branch, Corporate Services

- Director, IT Partner Management and Infrastructure Solutions Practice, Information Technology Branch, Corporate Services
- Cyber Security and Protection Sub-Committee, Information Management Committee
- Application/Information Owners
- Information Custodians

The following outlines the organization of cyber security and describes the roles, responsibilities and accountabilities for each. Roles, responsibilities and accountabilities for Application/Information Owners and Information Custodians are described in section 4.1.2.

General Manager, Corporate Services

The General Manager, Corporate Services is accountable for:

- Championing all aspects of cyber security in the City of Edmonton;
- Providing a cyber security program, strengthening cyber security systems that enhance the security and integrity of information technology; and
- Communicating and building awareness of cyber security issues, directive instruments and risks to Corporate Leadership Team.

Branch Manager, Information Technology Branch, Corporate Services

The Branch Manager, Information Technology Branch, Corporate Services is responsible for:

- Overall management, coordination and implementation of cyber security through the IT Security and Risk Assurance Program;
- Ensure that cyber security is included as part of Information Technology Branch activities;
- Setting IT Branch standards, technical standards and guidelines for cyber security;
- Communicating and building awareness of cyber security issues with peers and senior staff; and
- Ensuring that cyber security risks are identified, documented, and managed effectively to an acceptable tolerance level.

Program Manager, IT Security and Risk Assurance, Information Technology Branch, Corporate Services

The Program Manager, IT Security and Risk Assurance leads the IT Security and Risk Assurance Program. The program manager will:

- Be responsible for overseeing all aspects of security for information technology systems including monitoring and reporting compliance with cyber security guidance;
- Define and implement an cyber security strategy;
- Direct IT Branch staff to implement security controls or take specified actions to resolve security vulnerabilities or counteract threats;
- Monitor and respond to threats and risks that impact the security of City of Edmonton information technology systems;
- Provide a standardized framework for risk assessments and

management of security risks to information technology systems;
- Ensure risk assessments are completed on information technology systems and provide risk management recommendations to the Branch Manager Information Technology;
- Develop and deliver a program to maintain cyber security awareness and training;
- Being the single point of contact for cyber security issues and related concerns in the Branch; and
- Providing security advice and expertise to Departments and Branches.

Director, IT Partner Management and Infrastructure Solutions Practice, Information Technology Branch, Corporate Services

The Director, IT Partner Management and Infrastructure Solutions Practice, Information Technology Branch is responsible for:
- Developing and implementing an cyber security operations program for the Branch which complements the Corporate cyber security program;
- Actively monitor and respond to threats and risks that impact the security of information technology systems;
- Develop processes or procedures that supplement cyber security guidance; and
- Two-way communication of security challenges and issues with members of the Branch leadership team, the Corporate Services leadership team, Branch Managers and Directors.

Cyber Security and Protection Sub-Committee, Information Management Committee

The Cyber Security and Protection Sub-Committee is a forum for:
- Collaborating on cyber security activities;
- Discussing common cyber security issues;
- Sharing knowledge and enhancing cyber security competencies; and
- Coordinating cyber security activities on a City-wide level.

4.1.2. Cyber security roles and responsibilities must be defined for information technology systems.

4.1.2.1. Implementation Expectations

Application/Information Owners

Application/Information Owners should be assigned for all information technology systems. Application/Information Owners have the responsibility and decision making authority for the respective information technology systems throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.

Application/Information Owners will:
- Determine business requirements including cyber security needs and information classification;
- Ensure information technology systems are protected commensurate with their classification and value;
- Define security requirements during the planning stage of any new or

significantly changed systems;
- Determine authorization requirements for access to information and information technology systems;
- Approve access privileges to information maintained by the systems for each user or set of users;
- Ensure that authorized user lists are maintained current; and
- Be involved with security reviews and/or audits.

Information Custodians

Information Custodians maintain or administer information technology systems on behalf of the Application/Information Owner by:
- Providing and managing security for the systems throughout its lifecycle;
- Assisting in design and implementation, maintenance and operation of the technical infrastructure ;
- Assisting in design and implementation, maintenance and operation of the security infrastructure protecting information technology systems;
- Implementing and administering appropriate security measures to enhance and maintain a level of cyber security and control consistent with requirements; and
- Providing advice to Application/Information Owner on legislative and directive requirements for cyber security.

Information Custodians may be referred to as “Administrators”, “Application Administrators”, “Information Administrators”, “Infrastructure Administrators”, “Application Super Users”, or “System Administrators” in some communities of practice.

4.2. External Parties Technical Standard

4.2.1. Assessment of risk from external party access to information technology systems should be undertaken and appropriate cyber security controls implemented.

4.2.1.1. Implementation Expectations

The IT Branch should assess the business requirements and associated risks related to external party access to information technology systems. The assessment of risks related to external party access should consider:
- Impacts to the controls of the information technology systems;
- The classification of the information technology systems and the classification of the information associated with that systems;
- Internal and external processes for managing and reporting security and privacy incidents;
- Processes for identifying, authorizing, authenticating and reviewing access rights of personnel and systems of the external party; and
- Security controls to be used by the external party when storing, processing, communicating, sharing or exchanging information.

Prior to authorizing access by external parties to information and information technology systems it should be confirmed that:
- A risk and controls review has been completed and identified risks have

been mitigated or accepted;
- Residual risks will be monitored;
- The terms and conditions of access are documented;
- Responsibilities for managing and monitoring the external party access have been assigned, accepted and documented; and
- Security controls have been implemented and tested.

4.2.2. Security requirements must be identified and addressed prior to granting external parties access to City of Edmonton information technology systems.

4.2.2.1. Implementation Expectations

Refer to 4.2.1.1.

4.2.3. Arrangements involving external party access to City of Edmonton information technology systems must be based on a formal contract containing necessary security requirements.

4.2.3.1. Implementation Expectations

Refer to 4.2.1.1.

5. Reference

Further information can be found in:

- ISO 27002, Chapter 6 – Organization of Information Security