Information Technology Branch
Communications and Operations Management Technical Standard

Information Management,
Administrative Directive A1461

Cyber Security Technical Standard # 4

November 20, 2014

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

1. Purpose

This technical standard identifies the requirements to ensure that communications and operations functions of Information Technology Branch systems 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. Operational Procedures and Responsibilities Technical Standard

4.1.1. Operating procedures and responsibilities for IT Branch systems must be authorized, documented, and maintained.

4.1.1.1. Implementation Expectations

Operations documentation should be developed that is:

- Reviewed and updated annually; and
- Reviewed and updated as part of any related security incident investigation.

Operations documentation should contain instructions regarding:

- Systems re-start and recovery;
- Back-up and recovery;
- Exception handling;
- Audit and systems log management;
- Change management; and
- Operations, technical, emergency and business contacts.

4.1.2. Duties and areas of responsibility are to be segregated where possible to reduce opportunities for unauthorized modification or misuse of IT Branch systems.

4.1.2.1. Implementation Expectations

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of information technology systems. Care should be taken that no single employee can access, modify and use information technology systems without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Organizational size and structure may make segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision can be considered.

4.1.3. Development, test, and production environments for IT Branch systems are to be separated where possible to reduce the risks of unauthorized access or changes to the production environment.

4.1.3.1. Implementation Expectations

The level of separation between production, test, and development environments that is necessary to prevent production problems should be identified and appropriate controls implemented.

Appropriate controls can include:

- Separating production environments from test and development environments using different servers, domains and partitions;
- Users using different user profiles for production and test environments, with clear indications which profile is in use;
- Using approved change management processes for promoting software from development/test to production environments; and
- Restricting the use of production data in development, test or training environments where prohibited.

4.2. Third Party Service Delivery Management Technical Standard

4.2.1. Prior to using information technology systems and services external to the City of Edmonton, security controls, service definitions and delivery levels must be identified and included in the agreement with the external party.

4.2.1.1. Implementation Expectations

Security requirements should be included in procurement documents related to the acquisition of information technology systems and services (including “cloud-based” services) which are to be delivered by external parties.

Service definitions and delivery levels with external parties should be documented and include processes for:

- Ongoing review of service level needs;
- Audit and compliance monitoring rights and responsibilities (including security requirements and responsibilities);
- Communicating requirements to service providers;
- Obtaining periodic confirmation from service providers that adequate capacity is maintained; and
- Reviewing the adequacy of the service provider’s contingency plans for responding to disasters or major service failures.

4.2.2. Services, reports and records provided by external parties should be regularly monitored and reviewed.

4.2.2.1. Implementation Expectations

Processes should be established to manage and review the cyber security of external party delivered services by:

- Maintaining an inventory of agreements and associated access rights;
- Monitoring for compliance through processes such as:
  - Conducting internal self-assessments of control processes,
  - Requiring external parties conduct and submit self-assessments,
  - Requiring external parties to submit annual management assertions that controls are being adhered to, and
  - Conducting independent security reviews. .
- Establishing a process, jointly with the service provider, to monitor and evaluate cyber security incidents.

4.3. Protection against Malware Technical Standard

4.3.1. Preventive and detective controls must be utilized to protect IT Branch systems against malware such as viruses, spyware and ransomware.

4.3.1.1. Implementation Expectations

Anti-malware software should be implemented where appropriate at various points through the technical infrastructure.

4.4. Network Security Management Technical Standard

4.4.1. A range of controls must be implemented to achieve and maintain security within the City network as managed the IT Branch.

4.4.1.1. Implementation Expectations

Network infrastructure security controls and security management systems for networks should be implemented to maintain the protection of information and associated information technology systems.

To maintain the integrity of networks, network device configuration information such as configuration data, access control definitions, routing information and passwords should be managed and controlled.

Responsibilities and procedures for operational management of network infrastructure, including devices at network boundaries and in user areas should be documented.

To facilitate monitoring, response and investigation, logging to a log management service should be enabled and can include logging of:

- Traffic traversing network security boundaries;
- Traffic within networks housing sensitive or mission critical information, information technology systems;
- Security-relevant events on network devices; and
- Security-relevant events on security management technologies that provide authentication and authorization services to network infrastructure devices such as routers, firewalls or switches.

Network security controls should be documented and include:

- Roles and responsibilities for network security management;
- Specific procedures and standards used to mitigate risks and protect the network;
- Communication procedures for security-relevant events and incidents; and
- Monitoring procedures (including monitoring frequency, review and remediation processes).

4.4.2. Security features, service levels and management requirements of network services must be documented and included in any network service agreement.

4.4.2.1. Implementation Expectations

Formal network service agreements should be established between network service providers and consumers of network services to specify service levels, services offered, security requirements and security features of network services.

The network service agreement should include specification of:

- The rules of use to be followed by consumers to maintain the security of network services;
- The schedule for ongoing verification of network security controls;
- The rights of either party to monitor, audit or investigate as needed; and
- Security incident response responsibilities, contacts and procedures.

4.5. Media Handling Technical Standard

4.1.1. Portable IT Branch equipment must be protected using documented security controls.

4.1.1.1. Implementation Expectations

The IT Branch should ensure that portable IT Branch equipment such as laptops, tablets and other devices are protected commensurate with the value of the equipment and the sensitivity of the information. The following items are recommended for consideration to protect portable equipment:

- Sensitive data is encrypted;
- Equipment is protected from unauthorized access by the use of logical or physical access controls;
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate; and
- Personnel are familiar with operation of the protection technologies in use.

To provide further protection personnel can be instructed to:

- Not leave portable equipment unattended in a public place;
- Ensure that equipment is under their control at all times when travelling;
- Use the physical locking, restraint or security mechanisms whenever possible;
- Not permit unauthorized persons to use the equipment; and
- Report loss of equipment immediately.

4.1.2. When IT Branch hardware and media are destroyed, information must be protected against unauthorized disclosure.

4.1.2.1. Implementation Expectations

Information, records and software should be protected against unauthorized disclosure when hardware and media are destroyed following the guidance from the Corporate Records and Information Services practice in the Office of the City Clerk.

Where hardware and media is destroyed by third parties there should be contractual procedures to ensure complete destruction of the hardware and media. Third parties should certify that destruction has occurred. The IT Branch is responsible for ensuring hardware and media is destroyed using methods that are secure.

4.6. Monitoring Technical Standard

4.6.1. Audit logs recording user activities, exceptions and cyber security events with IT Branch systems must be produced and retained to assist in access control monitoring.

4.6.1.1. Implementation Expectations

Audit logs should be used to record user activities, exceptions and cyber security and operational events including information about activity on networks, applications and systems. The degree of detail to be logged should be based on the value and sensitivity of information assets, the criticality of the system and the authorized resources required to review and analyze the audit logs.

Audit logs may contain confidential data and access should be restricted to Employees with 'need-to-know' privileged access.

Audit logs should be retained according to the approved records retention schedule as established by the Corporate Records and Information Services practice in the Office of the City Clerk for the information, application, or infrastructure.

Audit logs may be configured to alert someone if certain events are detected. Alarm response procedures should be established and documented to ensure alarms are responded to immediately and consistently.

4.6.2. The use of IT Branch systems must be monitored and the result of the monitoring activities must be regularly reviewed.

4.6.2.1. Implementation Expectations

The use of information technology systems should be monitored to detect activities including: authorized and unauthorized accesses, and alerts and

failures. Specific activities should be identified to be reported as part of an exception reporting process.

Audit logs should be reviewed based on the assessment of the value and sensitivity of the information assets, the criticality of the systems and the resources required for review.

5. Reference

Further information can be found in:

- ISO 27002, Chapter 10 – Communications and Operations Management