EDMONTON

INFORMATION MANAGEMENT STANDARD

DIRECTIVE TITLE	DATE	*NOVEMBER 20, 2014*
INFORMATION MANAGEMENT, A1461	**DELEGATED AUTHORITY**	***BRANCH MANAGER, INFORMATION TECHNOLOGY***

STANDARD TITLE

CYBER SECURITY MANAGEMENT

DEFINITIONS

All definitions contained in the Information Management Administrative Procedure, A1461, apply to this Information Management Standard. For the purpose of this Information Management Standard, the following definitions also apply:

Cyber Security Technical Standards – the procedural documents describing Employee obligations and responsibilities for securing electronic City Information, listed in Attachment 1 and which form part of this Information Management Standard.

GUIDELINE

The Branch Manager, Information Technology, is responsible for developing, reviewing, and providing advice on Cyber Security Technical Standards necessary to ensure appropriate use technology solutions by the City. The Branch Manager, Information Technology, will regularly review the Cyber Security Technical Standards and provide advice on amendments or new Technical Standards on a regular basis to respond to changes in technology solutions used by the City.

The General Manager, Corporate Services, is responsible for approving and implementing the Cyber Security Technical Standards. The General Manager, Corporate Services, may also approve changes to Attachment 1 necessary to reflect the title and content of current Cyber Security Technical Standards. Any other changes to this Information Management Standard must be approved by the City Manager.

Employees must secure City Information by adhering to the Cyber Security Technical Standards.

Development and Implementation of Cyber Security Technical Standards

All Cyber Security Technical Standards will incorporate a risk-based approach to security using security threat and risk assessments supported by a set of baseline security controls applied consistently across the City. This approach must consider:

- business process and City service delivery implications;
- technological implications; and,
- communications strategies, including changes to Employee information security awareness programs.

THE CITY OF Edmonton

The risk-based approach must enable:

- compliance with legislative and policy objectives;
- business stakeholders to identify impacts to be considered;
- cost-effective allocation of resources based on a risk assessment;
- responsible governance of information technology systems and associated City Information;
- an enterprise view of risks relevant to all information technology systems; and
- secure provision of City information technology services.

When developing and implementing the Cyber Security Technical Standards, or when a particular City Information security issue is not explicitly addressed in the Cyber Security Technical Standards, steps taken to secure that City Information will be guided by the following principles:

1. **Support the business**

    - Focus on the business to ensure that securing City Information is integrated into essential business activities.
    - Deliver quality and value to stakeholders to ensure that information security delivers value and meets business requirements.
    - Comply with relevant legal and regulatory requirements to ensure that statutory obligations are met, stakeholder expectations are managed, and civil or criminal penalties are avoided.
    - Provide timely and accurate information on information security performance to support business requirements and manage information risk.
    - Evaluate current and future information threats to analyze and assess emerging information security threats so that informed, timely action to mitigate risk can be taken.
    - Promote continuous improvement in information security to reduce costs, improve efficiency and effectiveness, and promote a culture of continuous improvement in information security.

2. **Defend the business**

    - Adopt a risk-based approach to ensure that risk is treated in a consistent and effective manner.
    - Protect sensitive information to prevent disclosure to unauthorized individuals. City Information should be identified, classified, and managed according to its level of confidentiality.
    - Concentrate on critical business applications to prioritize scarce information security resources by protecting the business applications in which a security incident would have the greatest business impact.
    - Develop systems securely to build quality, cost-effective applications on which business people can rely.

3. **Promote responsible information security behavior**

    - Act in a professional and ethical manner to ensure that information security-related activities are performed in a reliable, responsible, and effective manner.
    - Foster an information security-positive culture to provide a security influence on the behavior of end users, reduce the likelihood of security incidents occurring, and limit their potential business impact.

STANDARD TITLE	DIRECTIVE	INFORMATION MANAGEMENT
CYBER SECURITY MANAGEMENT	DATE	*NOVEMBER 20, 2014*

Cyber Security Technical Standards

Attachment 1	**Information Technology Branch Organization of Cyber Security Technical Standard** Identifies the requirement to ensure that organizational roles and responsibilities for cyber security management are identified, implemented and managed following a set of baseline security requirements.
Attachment 2	**Information Technology Branch Asset Management Technical Standard** Identifies the asset management requirements for the management of information technology systems and the classification of information processed through those systems. Information technologies and information associated with those information technology systems form the assets that are the subject of this Technical Standard.
Attachment 3	**Information Technology Branch Physical and Environmental Technical Standard** Identifies the requirements to identify and manage physical and environmental threats against Information Technology Branch technology systems and the premises where those systems reside. This is achieved by establishing minimum controls for the physical security of technology systems.
Attachment 4	**Information Technology Branch Communications and Operations Management Technical Standard** Identifies the requirement to ensure that communications and operations functions of Information Technology Branch systems are identified, implemented and managed following a set of baseline security requirements.
Attachment 5	**Information Technology Branch Access Control Technical Standard** Identifies the requirement to ensure that access controls will be identified, implemented and managed appropriately for Information Technology Branch systems.
Attachment 6	**Information Technology Systems Acquisition, Development and Maintenance 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.
Attachment 7	**Information Technology Branch Cyber Security Incident Management 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.

STANDARD TITLE	DIRECTIVE	INFORMATION MANAGEMENT
CYBER SECURITY MANAGEMENT	DATE	*NOVEMBER 20, 2014*

Attachment 8

Information Technology Branch Business Continuity Management Technical Standard

Identifies the requirement to include cyber security requirements in the planning for the continuance of Information Technology Branch services where a human induced or natural disaster has occurred. This standard is not intended to provide overall direction and control for business continuity planning or coordination in the City.