

# **Information Technology Branch Asset Management Technical Standard**

**Information Management,  
Administrative Directive A1461**

**Cyber Security Technical Standard # 2**

**November 20, 2014**

**Approved:**

**Date:** November 20, 2014

## 1. Purpose

This 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 Standard.

## 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. *Responsibilities for Assets Technical Standard***

#### **4.1.1. *An inventory of all information technology and information associated with those systems should be documented and maintained.***

##### **4.1.1.1. Implementation Expectations**

The IT Branch should identify information technology and information associated with those systems in their custody or under their control.

Application/Information Owners and Information Custodians should document, maintain and verify asset inventories on a regular basis as

based on the criticality and value of the assets. Application/Information Owners and Information Custodians should also validate the measures taken to protect the assets.

***4.1.2. Application/Information Owners and Information Custodians should be designated for all information technology and information assets associated with those systems.***

**4.1.2.1. Implementation Expectations**

A master list of Application/Information Owners and Information Custodians should be developed and maintained.

***4.2. Information Classification Implementation Technical Standard***

***4.2.1. The Information Technology Branch will establish processes and procedures which implement the City of Edmonton information classification system.***

**4.2.1.1. Implementation Expectations**

The Branch Manager, Information Technology will establish processes and procedures to implement the City of Edmonton information classification system as established by the Corporate Records and Information Services practice in the Office of the City Clerk. The processes and procedures should take into account the value, sensitivity and intended use of the information.

Information Technology Branch processes and procedures should include guidance on:

- Making decisions on categorization of information;
- Applying people, processes and technology controls which are commensurate with the defined classification level;
- Periodic reassessment of the information categorization processes within the Information Technology Branch;
- Categorization of information technology based on the classification of information stored, handled or processed by the applications or infrastructure; and
- Inclusion of information security classification documentation in IT Branch security plans.

***4.2.2. Information should be identified, labeled where appropriate and handled in accordance with the assigned classification.***

**4.2.2.1. Implementation Expectations**

Where appropriate Application/Information Owners and Information Custodians should work with the IT Branch to label information technology, applications, infrastructure and information associated with those applications with the information classification. This allows users to

be aware of classification and protection requirements.

Application/Information Owners and Information Custodians should document handling procedures for secure processing, storage, transmission, and destruction of information. Any procedures should follow the guidance established by Corporate Records and Information Services practice in the Office of the City Clerk.

## **5. Reference**

Further information can be found in:

- ISO 27002, Chapter 7 – Asset Management