Information Technology Branch Business Continuity Management Technical Standard

Information Management, Administrative Directive A1461

Cyber Security Technical Standard # 8

November 20, 2014

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

1. Purpose

This 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 technical standard is not intended to provide overall direction and control for business continuity planning or coordination in the City of Edmonton.

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. Cyber Security Aspects of IT Branch Business Continuity Management Technical Standard

4.1.1. Managed processes are to be developed and maintained for business continuity throughout the IT Branch that address the cyber security requirements needed for the IT Branch's business continuity.

4.1.1.1. Implementation Expectations

The development of the IT Branch's business continuity planning process should involve the participation of the Program Manager, IT Security and Risk Assurance, Information Technology Branch.

4.1.2. Events that can potentially disrupt business processes within the IT Branch are to be identified, assessed for probability and impact to cyber security.

4.1.2.1. Implementation Expectations

IT Branch business impact assessment documentation should include a standard set of events which can disrupt processes and identify the impact to cyber security.

Identification of specific events should occur during the development of a business impact assessment, a risk assessment, and/or during the review or development of IT Branch business continuity plans.

4.1.3. IT Branch business continuity plans will be developed and implemented to maintain or restore operations in the required time frames following an interruption or failure of critical IT Branch processes.

4.1.3.1. Implementation Expectations

Plans should include requirements to ensure security of information and of information systems following an interruption or failure of critical IT Branch processes so that processes are upheld which meet assigned security levels.

4.1.4. IT Branch business continuity plans are to be tested and updated based upon criticality of the information or service.

4.1.4.1. Implementation Expectations

Testing of business continuity plan should include verification that cyber security requirements are being implemented.

5. Reference

Further information can be found in:

ISO 27002, Chapter 14 - Business Continuity Management