City of Burnaby

Meeting 2016 April 28

COMMITTEE REPORT

TO:	CHAIR AND MEMBERS FINANCIAL MANAGEMENT COMMITTEE	**DATE:**	2016 April 19
FROM:	CHIEF INFORMATION OFFICER	**FILE:**	1920-00

SUBJECT: **IT POLICIES**

PURPOSE: To provide members of the Financial Management Committee with details of the City's IT policies and staff awareness programs.

RECOMMENDATION

1. **THAT** the Financial Management Committee receive this report for information.

REPORT

1.0 BACKGROUND

Staff has recently updated the City's IT security policies in response to increased use of our network and business applications by citizens and employees, the evolving external security threat landscape and the need to attain – and retain – Payment Card Industry Data Security Standards (PCI-DSS) certification. The intent of these policies is to protect the City's IT infrastructure and data as new systems and services are rolled out; as well as to provide a review mechanism that will ensure policies continue to meet new security requirements. In addition to the general security policies listed below, each business application (e.g., SAP, Tyler EnerGov, ESRI GIS) has its own security framework which defines who can access what functionality within that system based on a user's job profile and required internal controls.

2.0 IT POLICY OVERVIEW

There are currently nine IT policies in place. Three are general policies intended for all users of the internal network, and six that are specific to IT technical staff.

The general IT policies are as follows:

- Acceptable Use of the City of Burnaby's Computing Technology and Network Resources
- Acceptable Use of the City of Burnaby's Email Systems
- IT Password Policy.

The IT staff-specific policies focus on the City's technical infrastructure and requirements to safeguard equipment and data. These policies are as follows:

- Standard Application Patching – to ensure critical security patches issued by vendors are applied to City servers
- Compliance Logging Control – to ensure City technology meets the PCI security standard and SANS Institute recommendations for event logging and management
- Physical and Infrastructure Security – covers security standards for data centre access
- User Identification and Passwords – covers software application access controls
- Controls for Viruses, Worms and Malware – covers the use of security tools and procedures to protect the City's network, systems and workstations from software-based security threats
- Network Security – covers the technology, processes and procedures to protect the City's network from external threats.

Due to the detailed technical nature of these IT-specific policies, access is restricted to IT staff. For the general policies, employee education and compliance is facilitated through: clear, user-friendly guides for work and home; publication of policies and guides on the staff intranet site; and availability of online training courses (with tracking capability) to validate employees' understanding. Specialized education is also provided for IT employees to ensure they stay abreast of security risk-mitigation strategies and technology.

The Clerk's department recently issued updated guidelines to ensure all staff understands how personal and confidential information should be handled at the City. And, in the context of social media, a Social Media Use policy and usage guide have been developed to provide staff with clear direction on how to represent themselves as City employees on-line.

Copies of the general City IT policies are attached to this report.

3.0 RECOMMENDATION

It is recommended that the Financial Management Committee receive this report for information.

Shari Wallace
Chief Information Officer

SJW:sjw

CC: Acting City Manager
Deputy City Manager
Director of Finance

City Clerk
City Solicitor