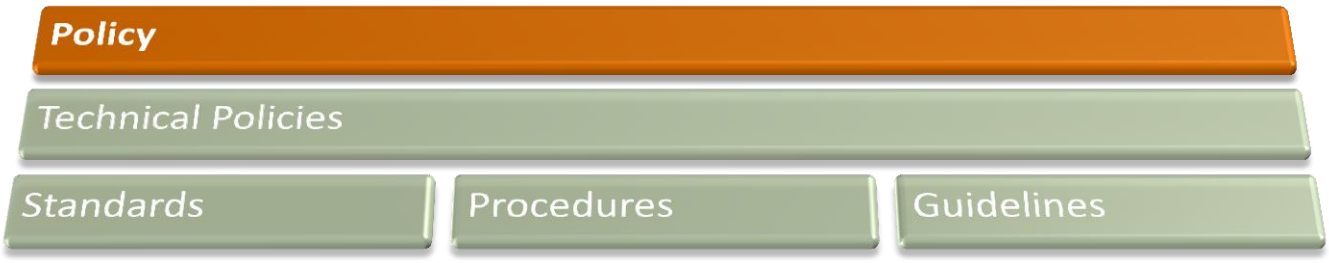
POLICY DOCUMENT

Policy Name: Information Security Policy	Department: Finance and Technology	Division: Information Technology
Doc ID = 451952	Author: Wendy Podgursky	
Policy Effective Date: July 1, 2009	Last Revision Date: May 5, 2014	



For a list of all policies and documents referenced in this policy, refer to the ***Document reference guide***, included in Appendix A.

Note that all policies and documents referenced appear in ***bold, italiced*** typeface.

1 SUMMARY

Those who utilize the City of Surrey's services entrust the City of Surrey (the City) with their personal information. The recent commoditization of personally identifiable information has called attention to the importance of planning, implementing and managing secure systems. The City is responsible to govern systems in a secure manner; ensuring that information is secure when it is obtained, transmitted and stored. The City is committed to retaining the confidence of the public and its employees in its approach to information management.

This policy defines the City's approach to managing electronic information security and electronic information systems protection, and communicates the responsibilities that all employees have for maintaining information security. This policy also provides a sound foundation for the City to build, maintain, upgrade, enforce and monitor secure systems and guide operational and implementation decision-making.

2 HOW TO USE THIS POLICY

This policy, which is available to all employees on the City's Intranet, will help identify the responsibilities that employees have when they work with information at the City of Surrey.

For information that is more specific to individual roles, refer to the policies, standards, procedures and guidelines for your division.

3 SCOPE AND APPLICABILITY

This policy applies to all levels of staff, acting in various roles within the City of Surrey and departments, including all management and employees. Details that are only applicable to a subset of employees have not been included in this high-level policy.

3.1 POLICY REVIEW SCHEDULE

The City shall review and update this policy annually, and as needed, if the scope or details of the policy change.

4 POLICY COMPLIANCE

Compliance with this security policy is mandatory. The City shall make this policy available on the City's Intranet for all employees and other individuals who may have access to the information and systems described herein. City employees shall be educated about security expectations in the form of login messages and through this policy.

All new employees must sign a letter agreeing to the City's ***Electronic Communications Acceptable Use Policy*** when they accept their offer of employment. To locate a copy of the ***Electronic Communications Acceptable Use Policy***, refer to the ***Document reference guide*** in Appendix A.

IMPORTANT: The City has the right to audit its systems to ensure compliance with this and other policies.

4.1.1 PCI COMPLIANCE

Failure to implement secure systems can result in incidents that negatively affect productivity and reputation and potentially expose the City to payment card industry fines and serious legal repercussions. The City created this document in tandem with an initiative for Payment Card Industry Data Security Standard (PCI DSS) compliance, as required to maintain our Level 3 Merchant status (organizations that process over 20,000 ecommerce transactions each year).

4.2 POLICY VIOLATIONS

Anyone who knows of or suspects a violation to this policy must report it immediately to the IT Service Desk using the it-servicedesk@surrey.ca e-mail address. The IT Service Desk will escalate the issue to the appropriate individuals for investigation and resolution. Repercussions for known policy violations may involve disciplinary action, termination of employment and/or legal action.

For questions regarding this policy, direct inquires to it-servicedesk@surrey.ca.

4.2.1 IMPLICATIONS FOR NON-COMPLIANCE

System users that do not comply with this policy will be subject to one or more of the following responses:

- Disciplinary action
- Termination of employment
- Legal action

5 INFORMATION SECURITY POLICY

5.1 USE AND OWNERSHIP OF INFORMATION

City communications systems and equipment, including e-mail and Internet systems, along with their associated hardware and software, must be used for official and authorized purposes only.

All City information is the property of the City, which may monitor, inspect, search, record or disclose any information or activities that occur on City resources. These resources are the property of the City and are subject to ***Freedom of Information and Protection of Privacy Act*** requirements should requests be made of City records. Users of City resources are not assured privacy with respect to use of these resources.

All content made available on the Internet, or on the City's Intranet, must be approved by and installed by the departmental content owners; this content is subject to the same Privacy Act and copyright restrictions.

5.1.1 ACCEPTABLE USE

Specific guidelines of acceptable use of e-mail, Internet, Intranet, mobile phones, telephone services, fax services and paging services, are outlined in the ***Electronic Communications Acceptable Use Policy***; City users must read and agree to this policy before using City resources.

All users receive a reminder of the ***Electronic Communications Acceptable Use Policy*** each time they login to a Windows workstation, which they must agree to before accessing City information systems.

> *REMINDER: This computer and the information created or stored on it are the property of the City of Surrey. The City may monitor, copy, access or disclose any information or files that you store, process, receive or transmit. All electronic records are subject to disclosure pursuant to the provisions of the Freedom of Information and Protection of Privacy Act, and pursuant to any demands for discovery of documents as part of a litigation process.*
>
> *The City has the right to audit its systems to ensure compliance with the City's Electronic Communications Acceptable Use Policy. For a copy of this policy, please see the City's Intranet.*
>
> *Keep your User ID and password confidential; do not share them. Remember that you are responsible for activities carried out under your User ID. For more information, review the Information Security Policy, which is available on the Intranet.*

5.1.2 UNACCEPTABLE USE

City employees must not use information in a manner that is designated as unacceptable. Unacceptable use of information includes the transmission of any materials in violation of Canadian laws including, but not exclusively:

- Duplicating, storing or transmitting pornographic materials
- Harassment
- Using vulgar, profane or inappropriate language
- Transmitting or posting threatening, abusive obscene material
- Duplication, storing or transmitting copyrighted material that violates copyright law
- Lobbying for political purposes,
- Operating a personal business,
- Participating in wagering, betting, in pyramid or chain schemes.

Users are bound by the City's conflict of interest by-law, ***City of Surrey By-Law NO 12196, article 4***.

5.1.3 CONFIDENTIALITY

City users must take precautions to protect City information, and make all possible efforts to maintain the confidentiality of personal information, business information and other proprietary informational resources.

Personally Identifiable Information (PII) shall be classified as confidential, as shall any other information flagged as such. City users must not transfer or store confidential information in any location not previously approved and secured by the City's Information Technology Division.

City information must not be stored on the local hard drive of any workstation, but stored only on provided, network-based locations.

Information Technology Division staff must provide access to information using the principle of least privilege, and shall provide access to informational resources on a need-to-know basis.

5.1.4 PERSONNEL SCREENING

The City must screen all candidates who are considered for sensitive and security-critical roles. New hires must satisfactorily complete screening, including a criminal record check, before being offered employment. For more information, refer to the ***Employment Checks Administrative Policy***.

Upon termination of employment, including the completion of any contract position, Infrastructure Services is responsible for disabling all of the departing employee's user accounts.

5.1.5 USE OF PHYSICAL AND INFORMATIONAL RESOURCES

City of Surrey resources shall be used for business purposes only; limited personal use is acceptable, if not excessive, and must not violate the terms of the ***Electronic Communications Acceptable Use Policy***.

5.1.5.1 NON-STANDARD SOFTWARE

Installation of software that is not on the City's approved software list is prohibited. Information Technology Division staff must configure all City workstations and is responsible for preventing the unauthorized installation of software.

5.1.5.2 NON-STANDARD HARDWARE

Information Technology Division staff must approve and configure any device that processes or transmits data. Hardware not issued or approved by the Information Technology Division is prohibited.

5.1.5.3 WORKSTATION SECURITY

City users must lock their workstations before leaving them unattended to prevent access to sensitive information by unauthorized users.

5.1.5.4 HANDHELD, WIRELESS AND MOBILE DEVICES

Departmental managers and the Information Technology division must approve handheld, wireless and mobile devices; all such devices must be used in accordance with the City's ***Electronic Communications Acceptable Use Policy*** and with all security policies that may be implemented by the City's Information Technology Division.

5.1.6 INTERNET USE

City employee use of the Internet must not interfere with normal business activities, and must comply with the ***Electronic Communications Acceptable Use Policy***.

Note that the ability to connect to a Web site does not imply that users are permitted to view that site; the City may log any activity to verify compliance and security.

5.1.7 APPLICATION IMPLEMENTATION AND USE

5.1.7.1 CITY OF SURREY E-MAIL

City provided e-mail services must be used for business purposes only, and must not violate the terms of the ***Electronic Communications Acceptable Use Policy***. Note that the City may log any activity to verify compliance and security.

Employees must not forward or redirect City e-mail containing confidential information through Internet-based webmail services.

5.1.7.2 WEBMAIL

Accessing personal, Web-based e-mail (webmail) using City resources must not conflict with City interests or violate the City's ***Electronic Communications Acceptable Use Policy***. Note that the City may log any activity to verify compliance and security.

5.1.7.3 INTERNALLY DEVELOPED APPLICATIONS

All internally developed applications must adhere to industry guidelines for security and encryption standards.

5.1.7.4 INTRODUCTION OF NEW APPLICATIONS AND SERVICES

In accordance with section 69(5.3) of the *Freedom of Information and Protection of Privacy Act*, all public bodies must complete a Privacy Impact Assessment (PIA) for all new initiatives. If it is determined that Personal information is being collected, appropriate controls must be implemented to protect this information.

Assesments are to be completed and filed with the City's Record Manger.

5.1.8 SECURITY CIRCUMVENTION

City users must not try to test, circumvent or bypass any security measure implemented by the City using any hardware or software tools.

5.2 ACCESS CONTROL

5.2.1 USER ACCOUNT

Each employee shall be responsible for the actions completed by their user account. City users must keep their user accounts and passwords confidential; shared or group user accounts are not permitted.

If a user believes that their user account information may no longer be confidential, they must report it to the IT Service Desk immediately.

For information about user account passwords, refer to the City's ***Network Authentication: User ID and Password Policy***.

5.2.1.1 USER ACCOUNT PERMISSIONS

Users with elevated security access to City informational and system resources must require such access for their job. Requests for elevated access must include the business justification for the change.

5.2.1.2 TEMPORARY USER ACCOUNT

The IT Service Desk provides temporary user accounts to third party resources, such as contractors, consultants vendors and students. These temporary user accounts must be configured with attributes that allow them to be distinguished from permanent accounts. Temporary user accounts must be configured to expire after the term of association is complete.

5.2.1.3 USER ACCOUNT LOCKOUT

After a number of failed login attempts, a user account shall automatically be locked out. Users must contact the IT Service Desk to re-enable their user account. For additional information regarding account lockout, refer to the ***Network Authentication: User ID and Password Policy***.

5.2.1.4 USER ACCOUNT CHANGES

Managers must inform the IT Service Desk when an employee changes role or is no longer employed by the City, to allow Information Technology Division staff to modify or disable the user's account immediately.

5.2.2 FACILITIES SECURITY

City servers which process and store credit card data must be located in a controlled environment, with access limited to approved members of the information technology team. Proximity readers are required to control and log all access to such areas, and monitored video surveillance must be in place.

5.2.3 ONSITE IDENTIFICATION

All City employees must wear city-issued identification badges when working in areas where confidential information may be accessed or stored.

All guests shall sign in to a visitor log that must be provided at each site or division and they must wear visitor badges for the duration of their visit.

For additional information regarding the identification badges, refer to the ***City Security: Identification Program***.

5.3 NETWORK SECURITY

The City must plan and implement appropriate security controls to protect the information that traverses and is available on City networks.

5.3.1 EXTERNAL AND THIRD-PARTY NETWORKS

All connections between the City network and third party networks shall abide by the ***Third Party Network Connection Agreement***. For information about the ***Third Party Network Connection Agreement***, contact the IT Service Desk.

The Infrastructure Services Manager must be responsible for approving connections from the City network to external networks.

5.3.2 ENCRYPTION

The City requires that all cardholder data that traverses City networks shall be encrypted, as per PCI standards.

5.3.3 ANTIVIRUS

Users must report detected viruses or suspicious workstation behavior to the IT Service Desk, as these incidents may indicate the presence of malicious code. Users must not disable or otherwise obstruct the operation of the antivirus software installed on their workstations.

City users must be aware of the danger of receiving or transmitting viruses and malicious programs over network systems.

5.3.4 WIRELESS

All wireless networks must be approved and implemented by the Information Technology Division, and configured to use authentication and encryption security controls to protect data.

The public Internet access wireless network blocks access to City operational systems and is therefore, exempt from the authentication and encryption requirements of this policy.

5.3.5 FIREWALLS

The City must position firewalls between all internal networks and the Internet.

5.3.5.1 FIREWALL ADMINISTRATION

Only Administrators that are authorized by the Infrastructure Services Manager shall perform firewall administration. Administration tasks must be performed at the terminal or via a secure connection. IT Network Security Administrators must document all firewall configuration data.

Quarterly, the Infrastructure Services Team shall complete system integrity checks, including a review of external connections, and an audit of firewall logs.

5.3.5.2 FIREWALL EXCEPTIONS

The Infrastructure Services Manager must approve all firewall exception requests, and supervises all changes to firewall configuration, including the removal of unused firewall exceptions.

5.3.6 REMOTE ACCESS

Users must receive management and Information Technology Division authorization to remotely access City resources based on business need. Users remotely accessing City resources are bound by the same security policies as on-site users.

5.3.6.1 SECURID TOKEN

When accessing the remote access portal, a SecurID token is required. Users must keep their SecurID tokens private and treat them with the same confidentiality as passwords. If a user suspects a SecurID token has been lost or compromised, they must immediately report it to the IT Service Desk.

5.4 OPERATIONS MANAGEMENT

5.4.1 OPERATING ENVIRONMENT

The City network must be segmented to protect and isolate confidential resources. The City must conduct annual network penetration tests to ensure data security.

5.4.2 AUDITING

Information Technology Division staff must configure all servers and network systems to log activity. All critical servers must have supplementary monitoring tools or software installed. System Administrators must review audit logs regularly for symptoms that indicate abnormal or potentially intrusive activity.

The Infrastructure Services Manager must be responsible for responding to any suspicious symptoms and determining when system integrity checks of the network perimeter access control systems are required.

5.4.3 SYSTEM CONFIGURATION

The Information Technology Division must define and follow best practices for configuring and securing devices. For more information, refer to the City's ***Configuration Management Technical Policy***.

5.4.3.1 PATCH MANAGEMENT

Information Technology Division staff must maintain computing resources by regularly applying patches and updates, as per the ***Patch Management Procedure***.

5.4.4 DATA BACKUP

The City must maintain regular data backups for archival and disaster recovery purposes. All backup and archival copies of City information must be physically secured both on and offsite. For more information, refer to the ***Backup Process*** documentation.

5.4.5 CHANGE MANAGEMENT

The City must use a structured change management system that monitors, manages and implements system modifications in a controlled manner. For more information, refer to the ***Change Management Process Documentation.***

5.5 INCIDENT HANDLING

If a user suspects that any information or system may have been compromised, they must immediately report it to the IT Service Desk, using the it-servicedesk@surrey.ca e-mail address, to make sure that an appropriate and timely response can begin. The IT Service Desk shall inform the Infrastructure Services Manager immediately of any security incidents that warrant a timely response.
Employees must fully cooperate in the incident response administered by the City. For more information, refer to the City's ***Incident Response Plan***.

5.5.1 INTERNAL INCIDENTS

Users must report any anomalies in system performance or usage to the IT Service Desk. Information Technology Division staff shall review all incident reports for symptoms that might indicate intrusive activity, viruses or other potential threats, and investigate suspicious symptoms on a case-by-case basis.

5.5.2 EXTERNAL INCIDENTS

IT Network Security Administrators must configure all firewalls to log activity to allow for analysis. An IT Network Security Administrator shall be notified of any security alarms by e-mail or automated call-out to allow for immediate response.

5.6 TRAINING AND SECURITY AWARENESS

The City must provide education and training to all users regarding their role in maintaining information security. For more information, refer to the City's ***Security Awareness Program***.

5.6.1 TRAINING EXISTING STAFF

The City must provide access to security policy materials for all users.

5.6.2 TRAINING NEW STAFF

All new, full-time employees of the City must sign a letter, agreeing to the ***Electronic Communications Acceptable Use Policy*** in conjunction with their new user orientation, which includes Internet and other hands-on system training.

5.7 POLICY EXCEPTIONS

Any exceptions to the City's ***Information Security Policy*** must be submitted to the IT Service Desk using the ***Request for Exception to Information Security Policy Form***. All exceptions must be approved by the Infrastructure Services Manager and the business need for the exception documented. Any exception must have a defined expiration date.

6 APPENDICES

6.1 APPENDIX A: DOCUMENT REFERENCE GUIDE

Related internal policies and documents

Document name	Location	Maintained by
City of Surrey By-Law NO 12196, article 4	http://intranet/Department/HumanResources/Policies/Code of Conduct By-Law No 12196.pdf	City Manager
Electronic Communications Acceptable Use Policy	http://intranet/Department/HumanResources/Policies/Electronic Communications Policy.DOC	General Manager - HR
Employment Checks Administrative Policy	http://intranet/Department/HumanResources/Policies/Employment%20Checks%20-%20Administrative%20Policy.pdf	General Manager - HR
City Security: Identification Program	http://intranet/Department/HumanResources/Policies/ID Badges Guideline 21.pdf	General Manager - HR
Incident Response Plan	The City Intranet – Link TBD	Infrastructure Services Manager – IT
Security Awareness Program	The City Intranet – Link TBD	Security Team - IT
Network Authentication: User ID and Password Policy	http://infoshare.surrey.ca/livelink/livelink.exe/open/443443	Infrastructure Services Manager – IT
Third Party Network Connection Agreement	Contact the IT Service Desk	Infrastructure Services Manager – IT
Change Management Process Documentation	file://file-server1/infotech/intranet/practices/processes/Change%20Management/ChangeManagementProcess.pdf	Infrastructure Services Manager – IT
Configuration Management Technical Policy	IT division's internal Intranet – Link TBD	Operations Manager – IT
Backup Process	file://file-server1/infotech/intranet/practices/processes/Operation%20Management/Backup%20Process.pdf	Operations Manager - IT
Patch Management Procedure	file://file-server1/infotech/intranet/practices/processes/Operation%20Management/PatchManagmentProcedure.pdf	Operations Manager - IT
Request for Exception to Information Security Policy Form	http://infoshare.surrey.ca/livelink/livelink.exe/open/443220x	Security Team - IT

Related external documents

Document name	Location	Maintained by
Freedom of Information and Protection of Privacy Act	http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00	Government of British Columbia

6.2 APPENDIX B: GLOSSARY

Antivirus: Software used to prevent and remove computer viruses.

Cardholder data: Personal information about the holder of a credit card which may include name, card number, expiry date, verification number on back of card, signature and any other personally verifiable information.

Confidential: Available to approved audiences only.

Employee: All individuals conducting work for the City of Surrey including, full-time and part-time employees, temporary employees, contractors, and consultants who provide on or-offsite services for the City. Analogous with *user*.

Firewall: Device designed and configured to control and secure all network traffic between logically separate networks, for example between a corporate network and the Internet. Firewalls limit access to authorized users only, while protecting data and resources.

Guideline: A guideline is a general statement, recommendation or suggestion to help achieve a policy's objective. In some cases, guidelines are more commonly known as 'best practices'.

Intranet: Web site used to share information exclusively within an organization and is not accessible to the general public over the Internet.

IT Service Desk: Also known as the IT Help Desk.

Moneris: The City's banking partner, which processes credit card payments on behalf of the city, and requires that the City become PCI compliant.

Mobile Devices: Mobile devices may include laptops, netbooks, mobile phones, smart phones and other devices.

Mobile storage devices: Devices used to store data for transport.

PCI: Payment Card Industry; a term used to describe the Payment Card Industry Security Standards Council, a global forum that develops and implements security standards for cardholder data protection. https://www.pcisecuritystandards.org/.

PIA: A Privacy Impact Assessment (PIA) is an assessment of a current or proposed initiative (a system, enactment project, program or activity) to evaluate privacy impacts, including compliance with the privacy protection responsibilities under the Freedom of Information and Protection of Privacy Act (FOIPPA).

PII: Personally Identifiable Information, industry term used to describe personal data such as name, address and other identifying data.

Policy: A policy is a formal and brief high-level statement that outlines an organization's requirements or rules that must be met.

Procedure: A procedure outlines how to how to complete the steps to fulfill the requirement outlined in a policy.

SecurID token: A small device that randomly generates a six (6)-digit number used to provide two-factor authentication when accessing a network.

Standard: A standard is mandatory action or rule designed to support compliance to a policy, usually system-specific or procedure-specific requirements that must be met by everyone.

User account: Uniquely identify a single City of Surrey user. Also known as User IDs or accounts. A user may have more than one user account, if each provides access to a unique environment; for example, they may have one user account for Windows and a second user account to log in to a database application.

Virus: Software added to a computer unknown to its operator, often designed to utilize computer resources for ill or other intentions without the knowledge of the owner.

Visitor: Is any individual, such as a vendor, guest of an employee, or service personnel who needs to enter the facility for a short duration, usually not more than one day.

Webmail: E-mail accessible using an Internet Browser interface, such as Gmail or Hotmail.

7 SIGNOFF

Name	Date	Signature
Geoff Samson *Manager, Information Technology Services*	June 15, 2009	Approved
Terry Kohan *Infrastructure Services Manager*	June 15, 2009	Approved
Anthony Labistour *Director, Client and Application Services*	June 15, 2009	Approved
Nicola Webb *General Manager - HR*	June 15, 2009	Approved

8 POLICY REVISION HISTORY

Version #	Date of Change	Author	Description Of Change
451952	June 22, 2009	Wendy Podgursky	Document publication
	November 15, 2010	Terry Kohan	Annual Review for currency
	October 28, 2013	Terry Kohan	Annual review and update for currency
	October 29, 2013	Terry Kohan	Add information on completing PIA's
	October 31, 2013	Terry Kohan	Revise PIA information description and add definition of PIA