REGINA Infinite Horizons | City of Regina

Corporate Policy

Policy Title:	Applies to:		Reference #
Information Security Policy	All information assets that belong to the City of Regina or are held by the City of Regina and belong to an employee, an elected official or a third party.		N/A
Approved by:	**Dates:**		**Total # of Pages**
Technology Governance Committee	**Effective:**	01-JAN-2016	8
	Last Review:	03-NOV-2021	
	Next Review:	02-NOV-2022	
Authority:			
The Cities Act (Saskatchewan) and *The Local Authority Freedom of Information and Protection of Privacy Act (Saskatchewan)*			

1.0 Policy Objective

The purpose of the Information Security Policy is to ensure the protection of all information assets belonging to or held by the City of Regina and provide overall direction to all employees regarding matters of information security, including the maintenance of information confidentiality, integrity, and availability. This policy supports the overarching Information Governance Framework, specifically the Information Security pillar.

The City is responsible for keeping and maintaining information in accordance with *The Cities Act* (Saskatchewan). Pursuant to *The Local Authority Freedom of Information and Protection of Privacy Act* (Saskatchewan), the City is responsible for protecting personal, confidential, and third-party information. All employees have a responsibility to protect information assets from unauthorized access, modification, transmission, or destruction and maintain the information in an accessible format to meet operational needs and retention requirements.

Unauthorized access use or disclosure of sensitive, personal, or confidential information can damage the City's reputation and lead to financial losses. The City of Regina is committed to managing its information assets to support service delivery to its residents and provide efficient operations.

2.0 Scope

This policy applies to all information held by the City of Regina or held on behalf of the City. Employees or elected officials disclosing information or providing access to information must be aware of the level of sensitivity of the information they are providing. Employees or elected officials must ensure that appropriate privacy and security protocols are in place and adhered to.

3.0 Definitions

"*Act*" – *The Local Authority Freedom of Information and Protection of Privacy Act* (Saskatchewan). *The Cities Act* (Saskatchewan).

"Disclosure" – when information assets collected by the City are provided to a third party that is not part of the City of Regina.

"Employees" – in scope staff, out of scope staff, consultants, and all staff of third-party organizations doing work on behalf of the City.

"Information Assets" – information stored in any manner which is recognized as 'having value' to the City.

"Information Classification" – the classification level assigned by the City's Data Security Classification Policy, prescribing the degree of sensitivity of an Information Asset.

"Local Authority" – a municipality

"Personal Information" – a type of an information asset that includes any personal information about an identifiable individual. For example, it may include information about race, religion; family status, age, place of origin, employment or criminal history, financial information, health services number, driver's license number, address, and telephone number, the views, or opinions of someone about that person, information about the physical or mental condition of an individual, along with a host of other information.

"Record" – means a record of an information asset in any form and includes information that is written, photographed, recorded, digitized, or stored in any manner, but does not include computer programs or other mechanisms that produce records.

"Third Party" – means a person, including an unincorporated entity, other than an applicant (if requesting information from the City) or a local authority.

"Use" – when an information asset collected by the City is used for an identified purpose.

4.0 Information Security Policy

4.1 Guiding Principles

The Information Security Policy is guided by the following principles:

- Security is everyone's responsibility.
- Security is a process, not a product.
- Security requires a multi-layered defense strategy.
- Security is only as strong as its weakest link.

4.2 Information Security Controls

Information security controls are designed to protect the City of Regina's information assets as well as to ensure the City meets its legal and contractual obligations with respect to information security. Security controls can be physical,

technical or environmental. These controls should be applied based on the information classification and potential harm that could result from the inappropriate access to use, disclosure, or loss of the information asset. These controls should also be assessed when contracting out to a third party that could involve the storage of information assets at third party property.

4.2.1 Physical Information Security Controls

Physical Information Security Controls represent all measures that can be taken by the corporation or business area and employees to physically protect *information assets*. These may include such measures as:

- Restricted access to certain areas of a building
- Video surveillance
- Locked rooms
- Use of locking devices such as filing cabinets
- Positioning of documents or computer equipment to limit or restrict access
- Including physical protection in work processes such as a clean desk or document transportation guideline

4.2.2 Technical Information Security Controls

Technical information security controls (also called logical controls) are devices, processes, protocols, and other technical measures used to protect the confidentiality, integrity, and availability of electronic information assets. These may include measures such as:

- Logical access systems
- Encryptions systems
- Antivirus systems
- Firewalls
- Intrusion detection systems

4.2.3 Environmental Information Security Controls

Environmental information security controls are measures taken to control the physical environment of the information assets to prevent loss or damage. These may include measures such as:

- Temperature
- Humidity
- Lighting

If environmental controls are required to ensure the integrity and availability of information assets, the Facilities Building Services Department should be consulted as soon as possible.

When contracting the storage of information assets to a third party, environmental controls should be assessed for the location of servers, computer hardware, photographs, paintings, and other physical records.

4.2.4 Retention & Preservation

Data retention and preservation deals with the management of information for a pre-determined length of time. Different types of data require different retention timeframes. Electronic information, just like hard copy information from years past, still needs to be retained for certain time periods based on the following criteria:

- Legal requirements
- Business requirements
- Personnel requirements

4.2.5 Application of Information Security Controls to Classified Data

Information security controls are linked to the City's Information Classification Policy and Guidelines (Appendix A) by way of defining the following:

- Confidentiality – knowing that information assets can be accessed only by those authorized to do so
- Integrity – knowing that information assets are accurate and up to date and have not been deliberately or inadvertently modified from a previously approved version
- Availability – knowing that the key data and Information Assets can be accessed as required to meet legal and/or operational requirements

5.0 Information Security Incident Management

Information security incidents that may impact or threaten the integrity, confidentiality and/or availability of information assets must be reported immediately. For detailed information on reporting and managing information security incidents at the City, see the Information Security Incident Management Guidelines.

6.0 Threat Risk Assessments

The employment of new technologies, processes, or proposed new uses for existing technology should always undergo an information security threat and risk assessment, including a privacy risk assessment where warranted. The assessment will help identify if the new technology or process poses any kind of risk to the information assets it manages or identify other systems/technologies at the City that could be impacted from a security perspective as a result of the new use or proposed technology.

See Information Security Threat Risk Assessment Procedure and Template under Section 7.0. For more information contact the Service Desk.

7.0 Related Standards, Guidelines and Procedures

Detailed technical, physical, and environmental standards/guidelines/procedures provide more explicit direction on corporate requirements for information security. This section of the policy is updated on a regular basis and does not require a formal review and approval of the policy to be amended.

- Data Security Classification Policy
- Data Security Classification Guidelines
- Employee Pre-Screening Guidelines (*to be developed with People & Organizational Culture*)
- Information Security Threat and Risk Assessment Procedures and Template (*to be developed*)
- Information Security Incident Management Process(*to be de*
- Information Systems Business Continuity Management Guidelines (*to be developed*)
- Network Security Standard/Guidelines
- Remote Access/Telecommuting Standards (*to be developed*)
- Logging and Monitoring Standards (*to be developed*)
- Change Control Standards (*to be developed*)
- Managing Removable Media Guidelines (*to be developed*)
- Email and Internet Usage Guidelines
- Wireless Security Standard (*to be developed*)
- Physical Security protocols *(to be developed)*
- Information Management Policy (*to be developed*)

8.0 Roles & Responsibilities

- The Information Technology Governance Committee (ITGC) is responsible for the approval of the Information Security Policy.

- The Information Security Working Group will develop standards, guidelines, and procedures that support the Information Security Policy. They will be approved by the Director of Innovation, Energy & Technology, City Clerk and Director of Facilities Services. The Chair of the Working Group will update the ITGC on new standards/guidelines/procedures as they are implemented.

- Innovation, Energy & Technology and Corporate Information Governance are responsible for promoting compliance and awareness of the Information Security Policy, including related standards/guidelines/procedures. This could include corporate communications as well as training and education.

- All business areas are responsible for the development of necessary operational procedures in their areas that comply with this policy as well as the related standards/guidelines/procedures.

- Periodic audits may be conducted to determine the City’s compliance with this policy and will assist in the investigation of policy violations.

9.0 Reference Material

- *The Cities Act* (Saskatchewan)
- City of Regina Privacy Policy
- *The Local Authority Freedom of Information and Protection of Privacy Act* (Saskatchewan)
- City of Regina Employee Privacy Guidelines
- *Bylaw 2012-18, The Records Retention and Disposal Schedules Bylaw, 2012*
- Information Classification Guidelines
- Information Management Policy

10.0 Revision History

Date	Description of Change	(Re)-Approval Required (y/n)
Feb-22-2013	Initial Draft of Policy	N
Nov-6-2013	Final Draft of Policy for ITGC	Y
Dec-16-2015	Final Draft of Policy for ITGC	Y
Oct-03-2020	Revision	Y

Appendix A - The following table provides examples of where information security controls need to be implemented:

- Confidentiality – knowing that information assets can be accessed only by those authorized to do so
- Integrity – knowing that information assets are accurate and up to date and have not been deliberately or inadvertently modified from a previously approved version
- Availability – knowing that the key data and Information Assets can be accessed as required to meet legal and/or operational requirements

Information Classification	Definition	Examples
High Sensitivity	♦ Information that is deemed to be extremely sensitive; of the highest value to the City. information protected by statutes, regulations, or City policies; information that can be used to create an identity. ♦ Inappropriate access, use or disclosure could reasonably be expected to result in extremely serious personal injury/harm or extremely serious injury/harm to the City, including financial loss to the City or third party, loss of life and/or risk to public safety, damage to the City's reputation and integrity, major political or economic impact.	Confidentiality: a) Information relating to a sexual harassment claim b) Information relating to the case files of a major lawsuit c) Compromise of personal, medical or health information Integrity: a) Information systems used for testing water supplies that could result in loss of life or severe illness b) Extended loss of service resulting in the need to institute manual processes Availability: a) Crisis communications during emergencies b) Essential fire communications
Medium Sensitivity	♦ Information that is deemed to be sensitive within the City of Regina. ♦ Inappropriate access, use or disclosure could reasonably be expected to result in serious injury/harm to the City including loss of competitive advantage, loss of confidence in a City program, legal action, financial loss, damage to partnerships, relationships or reputation.	Confidentiality: a) Issues dealt with in a private committee session b) Disclosure of trade secrets or intellectual property Integrity: a) Financial transactions and payments b) Information could be used to commit fraud or identity theft Availability: a) Financial and management information systems.

Low Sensitivity	♦ Information that is used within the City and deemed to be sensitive outside of the City of Regina. ♦ Inappropriate access, use or disclosure could reasonably be expected to result in significant injury/harm to individuals or to the City including financial loss, negative impacts in services/performance levels and reputation.	Confidentiality: a) Tender submission of a successful bidder b) Status of a City's evaluation of a company product Integrity: a) Information assets relating to administrative information such as volume and type of customer orders b) Operational procedure assets relating to non-critical activities Availability: a) Denial of service resulting in online registration not being available
Public	♦ Information that is intended for unrestricted public disclosure and would not reasonably be expected to result in injury to individuals, third parties, or to the City.	Confidentiality: a) Information of public knowledge that is posted to Regina.ca b) Internal information of the City where release would have no legal effect Integrity: a) Posting the final council-approved bylaw to the web and not another version Availability: a) News and public announcements