City Bylaws, Policies and Procedures

While the *Freedom of Information and Protection Act* ("FOIP Act") provides the minimum requirements, The City of Calgary's ("The City") commitment to protecting privacy and personal information is also demonstrated through various policies and practices that set out how The City collects, uses and discloses personal information. Privacy and personal responsibility for information is included in The City's Code of Conduct.

Privacy Impact Assessment Policy

(GN-022, Effective 2007, Policy Owner: City Clerk's Office)

Privacy Impact Assessments ("PIAs") are required for all City projects, practices and Information Technology systems that involve the collection, use or disclosure of personal information. The PIA process enables The City to exercise due diligence to identify risks to the privacy of individuals and mitigate the risks by implementing preventative and corrective measures. The PIA process engages key stakeholders from various areas including Corporate Security and Information Technology to understand and identify any privacy, security or technical risks.

Procedures and Operational Toolkit

- Self Service forms and information on myCity
- Collaboration with other jurisdictions
- FOIP Program Administrators in every Business Unit
- Defined PIA intake, stakeholder engagement and PIA reports
- In-person privacy consultations
- Access to Information and Protection of Privacy Handbook

Acceptable Use of City Technology Resources

(IM-IT-002, Effective 2003, Policy Owner: Information Technology)

The purpose of this Administration policy is to provide clear direction and accountability for what The City expects regarding acceptable, ethical and safe uses and monitoring of City technology resources. This Administration policy was an initiative between Access, Privacy and Policy, Corporate Analytics and Information, Corporate Security and Information Technology to consolidate nine (9) existing Administration policies addressing aspects of information into one central policy. This Administration policy is meant to encourage the sharing of and access to information by City staff while mitigating legal, privacy and financial risk.

Procedures and Operational Toolkit

- Information Security Project Risk Assessment
- Cloud and Open Source Risk Value Assessment
- Security testing and auditing
- Information Technology Device Management Tools

City Bylaws, Policies and Procedures

Information Management and Security Policy

(IM-IT-003, Effective 2013, Joint Policy Owners: Information Technology, Corporate Security, Corporate Analytics and Innovation, City Clerk's Office)

The purpose of this Administration policy is to provide standardized, transparent governance for Information Management and Information Security at The City. This Administration policy was an initiative between City Clerk's Office, Corporate Analytics and Information, Corporate Security and Information Technology and is meant to encourage the sharing of and access to information while mitigating legal, privacy and financial risk.

Supporting this Administration policy is a suite of technical standards that dictate minimum technical controls for access and information systems within The City.

Standards

- Electronic Communication Standard
- Information Security Classification Standard
- Intellectual Property Standard
- Access and Sharing Standard
- Technical Control Library

Procedures and Operational Toolkit

- Information Security Project Risk Assessment
- Cloud and Open Source Risk Value Assessment
- Security testing and auditing

Protecting Cardholder Data

(GN-032, Effective 2011, Policy Owner: Finance and Supply)

The payment card industry (PCI), which includes VISA, MasterCard, and American Express (card brands accepted by The City) has established minimum security requirements that organizations must follow to protect cardholder data. The City must adhere to PCI Data Security Standards (PCI-DSS) to be considered PCI compliant. This policy addresses the compliance responsibilities for each business unit with a role to play within the PCI–DSS process. The City's Merchant Bank communicates with Treasury to provide any updates to PCI-DSS as they occur.

Procedures and Operational Toolkit

- Annual PCI Security Compliance Assessment completed by independent Qualified Security Assessor
- Mandatory PCI awarenes training completed annually
- Third Party credit card processing

City Bylaws, Policies and Procedures

Records Retention Practices (Bylaw 53M99, Effective 1999)

The City's Records Management Program ensures that all official records are retained until they have met operational, legal and fiscal requirements, at which time they are disposed of by destruction, deletion or transfer to the City of Calgary Archives.

Bylaw 53M99 is supported internally by the following City Clerk's Administrative policies:

- Records Disposition (GN-013(b)), effective 2007
- Records Management Program Mandate and Responsibilities (GN-011), effective 2007
- Vital Records Management (GN-014), effective 2007
- Archival Records Management (GN-017), effective 2007
- Electronic Records Management (GN-015(b)), effective 2007
- Transitory Records Management (GN-016), effective 2007