ADMINISTRATION POLICY:

Information Management and Security Policy

Policy Number:	**IM-IT-003**
ALT Report:	**ALT2017-1110**
Approved By:	**Administration Leadership Team**
Effective Date:	**2018/01/30**
Next Revision Due:	**2021/01/30**
Department / BU:	**Information Technology, Corporate Security, Corporate Analytics and Innovation, City Clerk's Office**

BACKGROUND

The City of Calgary (The City) recognizes that Information and Intellectual Property are core strategic assets, along with people, finances and infrastructure. City of Calgary Information Assets and Information Systems represent a considerable investment and play a key role in all City of Calgary operations, including most service delivery activities, and in all decision making and planning activities.

The management of Information requires all Authorized Users to adhere to Information Management and Information Security standards, procedures and technical controls to protect Confidentiality, Integrity and ensure Availability of Information Assets and Information Systems.

Information has varying degrees of sensitivity and criticality. Some types of City Information and systems require a higher level of protection or special handling. Defining appropriate accountability and security for Information ensures that the right Confidentiality, Integrity, Availability and privacy measures are in place to protect this Information.

The collection, use and disclosure of Personal Information is governed by the Alberta *Freedom of Information and Protection of Privacy Act* (FOIP Act). The City and its staff are subject to the provisions of the FOIP Act and must ensure that Personal Information is collected and managed in compliance with the FOIP Act.

Proper classification of Information supports The City's objective of transparency and accessibility of Information to the public. Security classification of Information is a critical component in identifying Information that can be made available for routine disclosure to the public or as part of Open Data initiatives.

PURPOSE

The purpose of this policy is to provide standardized, transparent governance for Information Management and Information Security at The City. This policy is meant to encourage the sharing of and access to Information while mitigating legal and financial risk.

This policy and its associated standards, procedures and technical controls provide direction on the appropriate management of all Information throughout the Information lifecycle. This includes, but is not limited to, creating, acquiring, storing, managing, accessing, using, distributing, disclosing, destroying, securing and classifying Information Assets and Information Systems.

All associated standards, procedures and technical controls shall be considered to be an extension of this policy and carry the same consequences for non-compliance.

DEFINITIONS

Authorized User: An individual who has been granted access to use City of Calgary Information Assets or Information Systems; Authorized Users may be internal users (City of Calgary employees) or external users. External users are defined as the public, citizens, contractors, consultants or service providers working on behalf of The City; members of Council and Council staff; the Mayor and staff of the Office of the Mayor; boards, commissions and committees appointed by Council; Calgary Police Service; civic partners; other governmental organizations and approved researchers.

Availability: The accessibility of Information and Information Systems to ensure minimal disruption of service.

Confidentiality: The state of keeping or being kept private; ensuring Information, documents, Data, etc. are limited to authorized persons only.

Data: Data is a broad term, but generally refers to facts, concepts or instructions in a formalized manner which should be appropriate for communication, interpretation or processing by human or electronic means.

Information: Any collection of Data that is processed, analyzed, interpreted, classified or communicated in order to serve a useful purpose, present facts or represent knowledge.

Information Asset: Information recognized as having value for the purpose of enabling The City to perform its business functions, thereby satisfying a recognized business requirement. There are many types of Information Assets. Information Assets can include Data and Intellectual Property.

Information Governance: The exercise of authority, control and shared decision making (planning, monitoring and enforcement) over the management of Information Assets.

Information Management: The means by which The City plans, identifies, creates, receives, collects, organizes, governs, secures, uses, controls, disseminates, exchanges, maintains, preserves and disposes of its Information; as well as any means through which The City ensures that the value of that Information is identified and utilized to its fullest extent.

Information Security: The means by which The City protects the Confidentiality, Integrity and Availability of Information, Information Systems and Data from damage caused by malicious attacks, misuse or unintentional actions.

Information System: Any set of components that is used to handle Information. Information Systems include applications, services or any other assets that handle Information.

Integrity: Refers to overall completeness, accuracy and consistency; ensuring no corruption or unauthorised modification when referring to Data, Information or Information Systems.

Intellectual Property: All property, works, reports, Data, compilations of Information, computer programs, written presentations, memoranda, research drawings, sketches, layouts, commercial material, working papers, documents, copy, ideas, photographs and negatives, films, videotapes, video, audio and audio-visual productions and other materials in all forms and however fixed, stored, expressed or embodied, created, developed, generated, authored or produced.

Official Record: Recorded Information, regardless of medium, created, received and maintained by The City as evidence of a business transaction, decision or activity, that has legal, operational, fiscal or archival value.

Open Data: Refers to the idea that certain Data should be freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control (Wikipedia). The City's Open Data catalogue is governed by a terms of use which outlines how the content of the Open Data catalogue can be used.

Personal Information: Recorded Information about an identifiable individual as defined in Section 1(n) of the FOIP Act.

Records Management: The application of systematic control over the creation, organization, maintenance, retrieval, storage and disposition of records in order to meet operational, legal and fiscal requirements.

Transitory Record: Recorded Information, in any media (including email), that has immediate or short-term usefulness, or is required for a limited time to complete a routine action or to prepare an Official Record. It is not required for legal, operational, fiscal or archival purposes.

POLICY STATEMENTS

1. SCOPE / EXCEPTIONS

1.1. This policy applies to all Authorized Users.

1.2. This policy applies to all Information Assets and Information Asset security systems, new or existing.

1.3. This policy applies to both electronic and hardcopy Information.

1.4. This policy does not apply to Information owned by external parties. These groups are responsible for governing the collection and use of their own Information.

1.5. This policy does not take the place of or supercede any current legislation or municipal bylaw.

2. RESPONSIBILITIES

2.1. Administrative Leadership Team

Changes to the Information Management and Security Policy are approved by the Administrative Leadership Team (ALT). The ALT has delegated responsibility for the periodic review and approval of the Information Management and Security Standards to the Information Management and Security Governance Committee (IMSGC).

2.2. Information Management and Security Governance Committee

The IMSGC is responsible for and makes decisions regarding Information Management and Information Security at The City per the IMSGC Terms of Reference. The IMSGC is responsible for the periodic review and approval of the Information Management and Security Standards associated with this policy. The primary responsibilities of the IMSGC are to:

- Facilitate the implementation of Information Management and Information Security policies across The City;
- Provide Information Management and Information Security related technical, regulatory and policy leadership, including approving and reviewing related standards; and
- Approve exemptions to this policy and hear appeals regarding decisions rendered by the Chief Information Security Officer relating to standards, procedures or technical controls under this policy.

2.3. Information Management and Security Working Group

The Information Management and Security Working Group (IMSWG) shall, at the direction of the IMSGC, develop and/or contribute to Information Management and Information Security policies, standards and procedures. Terms of Reference for the IMSWG detail the scope, role, membership and operating procedures.

2.4. Chief Information Technology Officer (CITO)

The Director of Information Technology (IT) acts as the CITO for The City and is responsible for:

- Ensuring that Information technology investment is aligned to the strategic goals of The City;
- Ensuring the Availability of systems and communication infrastructure for City technology users;
- Ensuring that Information Security design is part of all system and infrastructure architecture design;
- Developing a process to identify opportunities for Information sharing and embedding that process into IT development methodologies and business practices; and
- Ensuring that IT plans are in place to enable business continuity.

2.5. Chief Security Officer (CSO)

The Chief Security Officer acts as the Chief Information Security Officer (CISO) for The City and is responsible for:

- The protection of City of Calgary Information Assets;
- Authorizing and overseeing physical and Information Security;
- Overseeing an Information Security program;
- Ensuring Information Security continuity by identifying potential threats and vulnerabilities and providing direction and guidance to ensure assets and infrastructure remain secure, accurate and available;
- Leading the Information Incident Management process for all suspected or actual Information incidents; and
- Approving or denying exemptions to the associated standards, procedures and technical controls.

2.6. Enterprise Information Management (EIM)

The EIM Program is responsible for:

- Providing specialist advice relating to Information Management practices;
- Identifying opportunities for Information sharing and cross-collaboration on projects and initiatives;
- Providing leadership in developing the strategic direction of Information Management within The City in conjunction with the Corporate Records Management Program, Bylaw 53M99;
- Co-ordinating the development and implementation of Information Management practices including policies, standards, guidelines and procedures;
- Assisting departments to define and understand their responsibilities in relation to Information Governance;
- Coordinating with the Chief Information Technology Officer and the City Clerk’s Office to plan and implement Information Systems to effectively manage The City’s Information Assets and electronic records;

- Ensuring program and project managers complete an Access Impact Assessment and/ or a Privacy Impact Assessment (PIA) in compliance with the PIA Policy;
- Reporting on stewardship issues and audit results to the IMSGC as required; and
- Providing change management, mentoring and training related to Information Management and Information Governance disciplines.

2.7. Innovation, Data & External Access (IDEA)

IDEA is a division of Corporate Analytics and Innovation. IDEA facilitates access to, or exchange of, City Information Assets on behalf of The City while protecting The City's interest and mitigating its liability. City Information Assets include Data and Intellectual Property.

IDEA markets The City's Data and negotiates and manages licenses controlling third-party access. IDEA administers the Intellectual Property and Access and Sharing Standards.

2.8. City Clerk's Office

In accordance with *The Municipal Government Act* and other legislation, the City Clerk's Office offers a wide range of services to citizens, The City and Council including the following:

- Carrying out the duties of City Clerk, which is a designated officer under *The Municipal Government Act*;
- Recording the decisions of Council and its Committees;
- Ensuring that Council records (agendas, reports, minutes, bylaws and agreements) are accessible, protected and maintained in perpetuity;
- Acquiring, preserving and providing access to Archival Records;
- Coordinating Records Management activities throughout The City, including program development, training, governance and updates to the Classification and Retention Schedule; and
- Receiving and processing requests under *The Freedom of Information and Protection of Privacy Act* including Privacy Impact Assessments.

2.9. Corporate Records Management and Archives

The Corporate Records team is responsible for establishing and coordinating Records Management activities throughout The City and managing The City's Archives. The team ensures that The City is able to provide, protect and preserve its records, in any media, in order to meet operational, legal, fiscal and archival requirements. Specifically, the team is responsible for:

- Developing, implementing and maintaining policies, guidelines and procedures for the management of all records in support of the Corporate Records Management Program;
- Providing Business Units with advice and consultation to implement the program across all records / Information repositories at The City;

- Developing and providing training and support materials for all aspects of the Records Management Program;
- Managing the records disposition process;
- Managing archival records;
- Provisioning and maintaining the Corporate Records Classification and Retention Schedule (CRCRS); and
- Administering the Records Management Software.

2.10. Freedom of Information and Privacy (FOIP) Office

The City Clerk, appointed by City Council as "The Head" of The City for the FOIP Act, has delegated the Manager, FOIP the role of FOIP Coordinator for The City and delegated specific responsibilities to this position.

As the FOIP Coordinator at The City, the Manager, FOIP is accountable for:

- Managing the FOIP Office;
- Developing and implementing The City's policies and procedures regarding FOIP;
- Leading the FOIP Division staff in the delivery of FOIP program services, products, activities and initiatives;
- Developing annual plans and reporting on key performance indicators to management;
- Coordinating the report of Issues Management and Risk Management;
- Overseeing that Section 38 of the FOIP Act is adhered to in the protection of privacy throughout The City;
- Overseeing the FOIP Office's prevention (i.e. Privacy Impact Assessment) and response (i.e. investigation programs related to allegations of privacy breaches), including the collaborative responses with Corporate Security;
- Ensuring that the FOIP Office provides timely expert advice to its clients and stakeholders, including the Administrative Leadership Team, Council, Departments / Business Units, etc.
- Responding to enquiries from the Office of the Information and Privacy Commissioner (OIPC) and / or Service Alberta regarding the FOIP activities throughout The City;
- Providing a City-wide FOIP training and outreach program to train and increase FOIP awareness throughout The City; and
- Liaising with the OIPC of Alberta and Service Alberta.

2.11. Managers and Supervisors

Managers and Supervisors are responsible for:

- Ensuring staff understand and adhere to this policy and its associated standards;
- Providing staff with access to this policy and its associated standards and procedures either in paper format or online;

- Ensuring staff are educated and aware of compliance requirements in relation to Personal Information in accordance with the FOIP Act and The City's policies;
- Ensuring employees are educated, aware and understand their Information Governance responsibilities and are empowered to fulfil them;
- Promptly following the Incident Response Procedure for all suspected or known violations of this policy and its associated standards. (All internal investigations are conducted by and the sole responsibility of Corporate Security.);
- Consulting with the IMSGC if, for any reason, they believe their staff cannot comply with the terms of this policy or its standards; and
- Promptly advising Innovation, Data & External Access (IDEA), a division of Corporate Analytics & Innovation, of any new, potentially high-value Intellectual Property developed.

2.12. Information Stewards

Information Stewards are the Authorized Users who are responsible for the management of specific Information Assets or Information Systems. Departments must ensure that Information Asset custodianship responsibilities are assigned to a role, not a physical person, so that they are maintained over time.

2.13. Authorized User

Authorized Users are responsible for:

- Understanding and adhering to the Information Management and Security Policy and its associated standards and procedures;
- Being educated and aware of compliance requirements in relation to Personal Information in accordance with the FOIP Act and The City's policies;
- Promptly advising Managers or Supervisors of any violation to this policy or its standards; and
- Promptly advising Managers or Supervisors if any portion of this policy or its associated standards are not understood or if, for any reason, they are unable to comply with this policy or its associated standards.

3. CONSEQUENCES OF NON-COMPLIANCE

3.1. Violations of this policy and its associated standards will be investigated by Corporate Security as directed by the CSO.

3.2. Internal Authorized Users who fail to adhere to this policy and its associated standards may be subject to disciplinary action up to and including termination of employment, seeking restitution, commencement of civil action, criminal prosecution or any combination thereof.

3.3. External Authorized Users who fail to adhere to this policy and its associated standards may have their access removed.

3.4. Contractors found to be in violation of this policy and its associated standards may be subject to suspension or termination of the contract.

4. POLICY STATEMENTS

4.1. GENERAL INFORMATION GOVERNANCE PRINCIPLES

4.1.1. Ownership: The City is the owner of Information

The City, as a legal entity, is the owner of all City Information Assets. No Authorized User, City department, business unit or division may 'own' City of Calgary Information.

4.1.2. Valued: Information is a core strategic asset

Information is a valued and strategic asset of The City and shall be managed, maintained and utilized to its fullest capacity.

- Information Assets shall be managed throughout their lifecycle; and
- Departments will routinely share and exchange Information amongst themselves and across departments to maximize the business value of Information Assets.

4.1.3. Managed: Information is actively planned, managed and compliant

The City is the custodian of a large and complex volume of Information that represents a significant investment and underpins the continued delivery of services. Department Information Governance practices must align with The City's administrative and Council policies and current legislative and regulatory requirements. Lack of compliance can lead to unforeseen risk and liabilities that could otherwise be avoided.

- Planning and investment arrangements for Information are formalized and apply City standards, methodologies and best practices;
- Departments have formal structures, responsibilities and procedural functions to govern Information throughout its lifecycle;
- Departments commit adequate resources to ensure that Information Governance activities and initiatives are successful;
- The compliance and audit requirements for Information Governance are consistent across departments, comprehensive, actively monitored and regularly reviewed;
- Proper Information Security controls as defined by Corporate Security are applied to Information and Information Systems to ensure Data Integrity and Availability;
- Departments are in compliance with The City's Corporate Records Management Program requirements.

4.1.4. Transparent: The public has a right to Information

The City holds significant amounts of Information. It is critical to an open, accountable and participatory government that the public has appropriate and reasonable routine access to general Information in the custody or under the control of The City. Recourse to the Freedom of Information and Protection of

Privacy (FOIP) Act is a legislated right and should be a matter of last resort in the context of increased proactive and routinely-released government Information.

The public has a right to access Information held by The City, with limited exceptions. It should be noted that this principle acts in concert with related legislation, regulation and administrative and Council policies. This not only supports increased openness, accountability and transparency, but a better-informed citizenry will be better placed to participate in the design and delivery of government services. Increased openness is a means by which The City can unlock the value of its Information resources to deliver better public services.

This principle extends to the exchange or sharing of Information between departments and even other governments, which improves efficiencies and reduces overall costs.

- Information collected at taxpayers' expense is made available to citizens to access wherever practical and appropriate, in accordance with legislation, administrative and Council policy;
- Departments must embed right to Information considerations in their business processes, actively planning for routine disclosure of Information to the public. Proactive and routine disclosure and right to Information considerations will underlie all Information decisions;
- Employees are educated and aware that the right to Information is a legitimate and core aspect of their work and they must work within the administrative and Council policies and legislation that govern this access;
- Clear licensing arrangements ensure that the public understands how they can use The City Information lawfully;
- Departments share and exchange Information amongst themselves and with other governments in accordance with administrative and Council policies;
- When sharing Information with other public bodies, a legal agreement is in place and costs to produce the Information may be recovered from the recipient public body;
- Recourse mechanisms (FOIP) are available to provide appropriate, transparent complaints and appeals processes.

4.1.5. Integrity: Information is accurate, relevant, timely, available and secure

Effective and valued government services must be trusted by their users. It is therefore essential that Information used for the delivery of services is of high quality and Integrity, and is managed in an ethical and accountable manner throughout its lifecycle to ensure it is accurate, relevant, timely, available and secure as appropriate.

- Information is collected, organized and stored in a manner that ensures its authenticity, quality and Integrity;
- Information should be relevant. It is collected for a purpose and to meet specific business or corporate requirements and outcomes;

- Confidentiality, privacy and security are considered for all Information decisions and are appropriately balanced against the right to access Information and compliance with legislation, regulation and administrative and Council policies;
- Mechanisms and procedures are in place to ensure appropriate Confidentiality, privacy, security and access processes are maintained and that these requirements are understood by all staff;
- Departments will work towards having a single corporate source of truth for key Information Assets;
- Retention and disposal of Information must be managed in accordance with The City's Corporate Records Management Program.

4.1.6. Private: Personal Information is protected in accordance with the FOIP Act

The City collects and holds significant amounts of Personal Information. Citizens and staff have a right to privacy and departments are responsible for ensuring that such Information is responsibly collected, used, disclosed and protected in accordance with the *Freedom of Information and Protection of Privacy (FOIP) Act.*

- Departments comply with Information privacy requirements according to the *Freedom of Information and Protection of Privacy Act* and embed them in their administrative practices;
- Citizens and staff have a right to privacy, with limited exceptions, and the right to access or request correction of their own Personal Information in The City's custody or under The City's control (as per the FOIP Act).

4.1.7. Equitable

Information should be equally accessible to all regardless of geographic, economic, social or disability situations. Information must be presented in a way that is intuitive to understand and use, as much as is practical.

- Arrangements exist to enable all to access The City's Information as equitably as is practical;
- Particular attention is made to ensure that Information is accessible to those who may in some way be disadvantaged economically, socially or through disability and in a way that does not create hardship;
- Information is made available in a manner in which it can be used by those it is given to. This leads to the need to present Information in different formats so that people who use the Information may choose the format that best works for them;
- Staff are educated and aware of the requirement that Information is to be accessible to all.

4.2. GENERAL POLICY STATEMENTS

4.2.1. Duty to Protect

Certain Information, such as citizen and staff Personal Information may be in the custody and control of The City. In cases where The City does not 'own' this Information, The City still has a legislated duty to protect it with the same care and attention as it would with its own Information. Users need to ensure that all Personal Information, regardless of who 'owns' this Data is secured against unauthorized access, collection, use, disclosure or destruction as defined in the associated Information Management and Security Standards and in accordance with Section 38 of the *Freedom of Information and Protection of Privacy Act.*

4.2.2. Information Governance

Information Governance functions will be required within departments to ensure compliance with relevant legislation, regulations, administrative policies and Council policies. This establishes an authorizing and accountability environment for the release of Information and develops Information Management and Information Security strategies and work plans which maintain and improve departmental Information Governance maturity.

4.2.3. Routine Disclosure

City of Calgary Information that meets requirements outlined in the associated Information Management and Security Standards will be made available to Authorized Users, including the public, either proactively or upon request.

4.2.4. Intellectual Property

Intellectual Property created by City of Calgary staff, as part of their job descriptions, or as a result of a formal direction from management, or created by contract personnel while employed by The City, is an Information Asset owned by The City. Management of Intellectual Property is described in the associated Information Management and Security Standards.

4.2.5. Information Security

Information Security activities and decisions are the responsibility of Corporate Security. Implementation of Information Security activities must be coordinated with and approved by Corporate Security. Applying appropriate controls, classification and security to Information and Information Systems is described in the associated Information Management and Security Standards and Technical Controls. Where a standard, procedure or technical control is silent, the CSO, at his or her discretion, will rely upon the current version of one of the following industry standards or existing practices:

- ISO IEC 27000 - 27004
- Payment Card Industry (PCI) Data Security Standards (DSS)
- NIST 800 and NIST Cybersecurity Framework

The CSO or his or her delegates in Information Security will bring the relevant sections of these standards to the attention of the appropriate parties when necessary.

4.2.6. Information Technology Assets / Inventory

Corporate Security, in conjunction with IT and all other business units utilising IT assets not stewarded by IT, will maintain an inventory of all Information Technology assets, namely applications (on-premise or off-premise, Cloud, mobile, etc.), hardware devices (servers, network devices, endpoint, intelligent controllers, mobile, etc.) and storage devices (real or virtual).

5. POLICY REVIEW

This policy shall be reviewed every 3 years. The associated standards to this policy will be reviewed annually by the IMSGC. This policy or the standards may be reviewed sooner if required due to changes in the business or the risk environment.

SUPPORTING REFERENCES AND RESOURCES

Please note that some of the items listed below may not be publicly available.

References Related to Corporate-Wide Procedures, Forms and Resources

- Information Management and Security Standards
- Information Management and Security Governance Committee (IMSGC) Terms of Reference
- Information Management and Security Working Group (IMSWG) Terms of Reference

References related to Council Policies, Bylaws and Administration Policies

- Privacy Impact Assessment (GN-022)
- Protecting Cardholder Data (GN-032)
- Records Management Program Mandate and Responsibilities (GN-011)
- Inactive Records Management (GN-012)
- Records Disposition (GN-013)
- Vital Records Management (GN-014)
- Electronic Records Management (GN-015)
- Transitory Records Management (GN-016)
- Archival Records Management (GN-017)
- Transparency and Accountability Policy (Council Policy CC039)
- Records Management Bylaw (53M99)

Other References and Resources

- *Freedom of Information and Protection of Privacy Act* (FOIP Act)

REVISION HISTORY

Review Date	Description
2018 / 01 / 30	Information Management and Security Policy (IM-IT-003) reviewed and amended (ALT2017-1110). New policy replaces: • IM-IT-003 Information Governance Policy (ALT2013-0734) • IM-IT-001 (A) Information Security Classification and Control • GN-018 (D) External Data Access Management • GN-019 Intellectual Property Management • GN-020-21 (A) 311 Data Management and Privacy • ALT2015-0865 Interim Information Security Policy
2015 / 11 / 17	Interim Information Security Policy reviewed and amended (ALT2015-0865).
2013 / 12 / 03	Information Governance Policy (IM-IT-003) reviewed and approved (ALT2013-0734).