INFORMATION MANAGEMENT AND SECURITY STANDARD

Information Security Classification

Approved By:	**Information Management and Security Governance Committee**
Effective Date:	**2018/01/30**
Next Revision Due:	**2021/01/30**
Department / BU:	**Corporate Security**

GENERAL

This standard is an extension of the Information Management and Security Policy. Consequences of non-compliance with this standard are outlined in the policy.

For the purposes of this standard, the terms 'information asset' and 'information' are used interchangeably. All City of Calgary information is a corporate asset.

PURPOSE

All information generated and maintained within The City of Calgary has varying degrees of sensitivity depending on the content and use of the information. The City's *Information Security Classification Standard* communicates the need for special handling measures that must be consistently applied to The City's information, irrespective of the information location or format of the information (hard copy or electronic).

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

SCOPE

This standard applies to all information, both hard copy and electronic, and information systems.

INFORMATION SECURITY CLASSIFICATION LEVELS

The three levels used to classify The City’s information are:

1. **Restricted** (Highest Level of Security)

“Restricted” describes information that has significant value to The City, and unauthorized disclosure or dissemination could result in injury or loss of life, significant financial harm or significant reputational damage. Due to its privacy, legal or competitive content, access to Restricted information is strictly defined and limited to only a few individuals. Information and the associated information systems designated to be of a Restricted nature must have security measures in place to protect them from unauthorized access, disclosure or modification in accordance with security measures dictated by the completion of the *Impact Assessment Procedure.*

2. **Confidential** (2nd Highest Level of Security)

“Confidential” describes information that has value to The City. Unauthorized disclosure or dissemination of Confidential information could lessen The City’s competitive advantage, reduce The City’s revenue-generating potential, disclose The City’s intellectual capital to potential competitors or cause reputational damage. Confidential information includes non-public, personal information that could cause financial or reputational harm to an individual, information that could cause economic loss and information that could significantly reduce the level of public trust in The City.

Information and associated systems designated to be of a Confidential nature must have protective security measures in place to prevent unauthorized access, disclosure or modification in accordance with security measures dictated by the completion of the *Impact Assessment Procedure*. Access to Confidential information can be made available to authorized users who have been granted authorization by the appropriate information steward.

3. **Unrestricted**

“Unrestricted” information is created in the normal course of business, and is unlikely to cause harm to individuals or to The City. The public release of Unrestricted information does not violate its confidentiality and does not reduce The City’s competitive business advantage, damage The City’s business reputation or hold The City accountable to any person, agency or organization.

Unrestricted information can be routinely made accessible to the public because adverse consequences are unlikely to result from wide-spread dissemination. Information classified as Unrestricted should be considered open (read-only to all City of Calgary staff) by default.

Classification	Examples	Risk
Restricted *Applies to limited amount of information.*	• Plans for sensitive facilities and critical infrastructures • Security procedures • Encryption keys	• Loss of life • Extreme or serious injury • Extreme impact to public safety • Catastrophic financial loss • Catastrophic damage • Sabotage and terrorism
Confidential *More common.* *Exists in large concentrations within certain Business Units.*	• Personal or financial information related to individual citizens or businesses • Highly-valued intellectual property • Materials prepared for in-camera Council meetings • Material subject to legal privilege • Testing and auditing procedures • Negotiation information related to suppliers and third parties • Contracts • Information pertaining to negotiations with provincial or federal government which could jeopardize relations with that government • Personnel investigations • Personnel files or information including an employee's medical history, complaints on their file, salary, pay for performance, police check information • Corporate credit card and customer credit card information	• Loss of reputation or competitive advantage • Loss of confidence in a City program • Loss of personal or individual privacy • Loss of trade secrets or intellectual property • Loss of potential revenue • Damage to partnerships
Unrestricted *Majority of information at The City.*	• Most internal correspondence (paper or electronic) • Published Council Meeting Minutes & Agendas • White papers • Meeting minutes	• Little or no impact • Minimal inconvenience if not available • Minimal financial loss

	• Fee schedules • Building permit files • Public Health and Safety information • Job titles, job descriptions, pay scales	

Default Information Security Classifications

Information is considered Unrestricted by default.

If information is not labelled with an information security classification, it is considered to be Unrestricted.

Multi-class Information

If the information system or information asset contains sections with different information security classifications, all efforts should be made to separate out and/or make available the portions that are Unrestricted. In the event the sections cannot be separated, then the higher level of classification and protection must be applied to ALL of the information.

INFORMATION HANDLING INSTRUCTIONS

Access to and Sharing of Information

The *Access and Sharing Standard* outlines the methods of internal and external sharing of City of Calgary Information Assets.

Storing Corporate Information

Information must be securely stored and protected in accordance with its security classification level.

Hard Copy Information

Classification	Storage Requirements
Restricted	• Restricted information must not be left unattended and must be locked in a secure filing cabinet or locked room when not in use
Confidential	• Must be locked in an office, desk or filing cabinet when desk is left vacant or outside of office hours
Unrestricted	• Should be stored out of plain sight when desk is left vacant or outside of office hours

Electronic Information

All City of Calgary information assets, systems and network access will be secured by Corporate Security and Information Technology.

Classification	Storage Requirements
Restricted	• Must be encrypted at rest in a defined and secure location • Access will be controlled and logged • Logging is to be enabled on all systems housing Restricted information; All logs are to be reviewed by Information Security and all anomalies are to be investigated • Restricted information will not be stored on local drives (C: drive of a laptop, tablet or PC), removable media or network drives (H: or S: drives)
Confidential	• Information will be stored in a defined and secure location (e.g. H: drive, Livelink) in accordance with the *Information Security Design Standard* • Confidential information will not be placed on local drives (C: drive of a laptop, tablet or PC), removable media or network drives (S: drives) • Access will be controlled and logged in accordance with the *Access Control Standard*
Unrestricted	• No special storage or security requirements • Information will be stored on appropriate network storage. (e.g. H: or S: drives) • Care must be taken to protect the integrity, accuracy, relevance and availability of unrestricted information published electronically to prevent unauthorized modification that could harm the reputation of The City

All City issued technology resources must be either continuously monitored or locked. Users are expected to secure the physical device in accordance with the provisions of the *Acceptable Use of City Technology Resources Policy*.

Information Handling Procedures

Information must be securely transmitted (electronic) or transferred (physical/paper) in accordance with its security classification level.

Classification	Print/Hard Media	Electronic Files
Restricted	• Tamper evident packaging (e.g., double-sealed envelope with inside envelope signed to reveal evidence of tampering) • Transmitted under a continuous chain of custody with receipts covering each individual who obtains custody	• Including Restricted information in electronic mail transmission (email) is prohibited if encryption e-mail options are not used • Restricted information should never be transmitted over external networks
Confidential	Sealed Confidential envelope	• Encryption must be used to protect Confidential information when it is transmitted to or from the external zones (untrusted networks) • Confidential information contained in or attached to electronic mail transmissions must be encrypted if sent to anyone outside of The City's network
Unrestricted	No special procedures	No special procedures

Information Labelling Procedures

Information Security Classifications need to be clearly identified on the information asset.

If the information contains sections with different information security classifications and the sections cannot be separated, then the higher level of classification and protection must be assigned to ALL of the information.

Type	Procedure
Hard copy documents	Rubber ink-stamps for each level to mark hardcopy documents as needed. It may be necessary to stamp each page in case the document pages become separated. Stamps can be ordered on-line at http://finsupply/purchasing/office_supplies.html and follow link under Rubber Stamps.
Electronic mail	Identify information security classification in subject line of e-mail, only if classified as Confidential. Transmission of Restricted information via email is prohibited unless encrypted.
Electronic documents	Identify information security classification in document metadata. If additional classification options are available as part of a document management system they should be employed as well. Information Security Classification should be marked clearly in the footer of all documents and appear on all pages. • The following is stored on the title page: ○ Information Security Classification (ISC) code ○ ISC Review Date: Anticipated date classification code may change or should be reviewed (optional) ○ Information Steward ○ Information Steward's Business Unit
Data, databases and business applications	Identify classification in system/application metadata. All application and databases housing Confidential or Restricted information should be properly secured and have appropriate protection.
Other media	Confidential or Restricted information must never be stored on removable media. Only Unrestricted information can be stored on removable media.

Disposition

Business Units are responsible for reviewing the ISC classification of their information assets and downgrading that classification (if appropriate) to “Unrestricted” before initiating the formal Corporate Records Disposition process. If records are still classed as “Confidential” or “Restricted” and can potentially become part of The City’s Archives, special handing will be required.

All information must be properly managed throughout its lifecycle (creation, use and disposal), according to the Corporate Records Management Program.

RESOURCES

Refer to the **Administration Policy Library** for the following:

Information Management and Security Policy

Corporate Records Management Policies and Program

REVISION HISTORY

Review Date	Description
2018 / 01 / 30	New Information Security Classification Standard reviewed and approved by Information Management and Security Governance Committee.