INFORMATION MANAGEMENT AND SECURITY

Information Security Classification Standard

Approved By:	**Information Management and Security Governance Committee**
Parent Policy:	**Information Management and Security Policy**
Effective Date:	**2022/12/13**
Next Revision Due:	**2025/12/13**
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.

PURPOSE

The City's Information Security Classification Standard specifies classification and protection measures that must be consistently applied to The City's Information Assets.

In addition to supporting The City's information security requirements, appropriate information classification supports The City's objectives of transparency, accessibility of information both internally and to the public, and by helping to identify 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 Authorized Users and all City of Calgary Information Assets.

DEFINITIONS

“Authorized User” means an individual who has been granted access to use City Information Assets or Information Systems; Authorized Users may be internal users (City employees) or external users;

“Availability” means the accessibility of Information and Information Systems to ensure minimal disruption of service;

“City-Managed” means Information Systems owned and operated by The City of Calgary or those operated by others in an approved contractual relationship with The City, whether on City premises or off-premises (i.e. cloud services);

“**Confidential**” means the information so classified is valuable or sensitive to The City or requires protection by law, regulation, agreement, or City policy;

“Confidentiality” means the state of keeping or being kept private; ensuring Information, documents, Data, etc. are limited to authorized persons only;

“Data” means any facts, concepts, quantities, characters, or instructions stored and/or transmitted in electronic formats;

“Information” means any collection of Data that is processed, analyzed, interpreted, classified, or communicated to serve a useful purpose, present facts, or represent knowledge;

“Information Asset” means 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. May be used interchangeably with “Information” in this standard.

“Information Steward” means any Authorized User given responsibility for the management of specific Information Assets or Information Systems.

“Information System” means any set of components used to handle Information. Information Systems include applications, services, or any other assets that handle Information;

“Integrity” means assurance of the accuracy and reliability of the Information and Information Systems is provided and any unauthorized modification is prevented.

“Intellectual Property” means all trademarks, copyrights, art, inventions, creative works, reports, Data, compilations of information, computer programs, 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;

“Personal Information” means the recorded information about an identifiable individual as defined in Section 1(n) of the Alberta *Freedom of Information and Protection of Privacy (“FOIP”) Act*

“**Restricted**” means the information so classified is of high value or sensitivity to The City and, if compromised, could put The City at financial or legal risk. Restricted classification of certain information may also be required by law, regulation, agreement, or City policy.

“Service Owner” means an individual responsible for representing the service on behalf of the Administration.

“**Unrestricted**” means the information so classified is unlikely to cause harm to individuals or to The City if released publicly. This is the default classification.

STANDARD DETAILS – CLAUSES AND SUBCLAUSES

ROLES AND RESPONSIBILITIES

Users

All Authorized Users of Information and Information Systems must:

- Classify Information they create in accordance with the requirements of this Standard
- Label all Information they create according to the three classification levels defined in this Standard
- Recognize the classification ratings assigned to Information Assets created by others and safeguard those assets accordingly
- Complete Information Security Classification training

Information Stewards

Information Stewards must:

- Manage specific Information Assets or Information Systems including ensuring that information they are responsible for is classified properly
- Take steps to secure Information Assets or Information Systems according to their classification level
- In the event of a classification change, ensure that Corporate Security is engaged for an analysis of security controls to determine whether existing security controls are consistent with the new classification
- If gaps are found in existing security controls, work with relevant groups (Information Technology, Corporate Security, City Clerk's Office, etc.) to address the resulting risk(s)

Service Owners

Service Owners must:

- Designate themselves or another Authorized User as the Information Steward for each service they are accountable for
- Identify the security classification level of all service-related information and Information Systems
- Reevaluate the classification of Information Assets as required by a change in the type of Information, change in business process or change in technology to ensure the assigned classification is still appropriate
- Maintain awareness of the security classification level and the effectiveness of implemented security controls, even if not acting as an Information Steward.

Managers and Supervisors

Managers and Supervisors must:

- Ensure that all their direct reports are made aware of this Standard and its corresponding guidelines
- Ensure that all direct reports understand the importance of classifying, labelling, and safeguarding Information
- Complete the Information Security Classification training and oversee its completion by all direct reports

Corporate Security

Corporate Security must:

- Maintain this Standard and the corresponding guidelines
- Provide Standard interpretation and guidance as required
- Provide tools to raise awareness about the requirements in this Standard and help all users meet their obligations to implement them
- Provide information security services as may be required to assist Business Units in the implementation of this Standard

Information Technology

Information Technology must:

- Provide, or assist with, electronic Information and document management practices as appropriate
- Work with Corporate Security to ensure that appropriate security tools and services are made available to enable the appropriate safeguarding of Information and Information Systems of all classification levels
- Provide hosting and storage environments that enable the appropriate safeguarding of Information and Information Systems of all classification levels

City Clerk’s Office

The City Clerk’s Office must:

- Work with Corporate Security and Information Technology to ensure legislative requirements under the *Freedom of Information and Protection of Privacy Act* (*FOIP*) and the *Municipal Government Act* are addressed in this Standard and related standards, procedures, and guidelines
- Coordinate the Corporate Records Management Program activities throughout The City

Collaboration Analytics & Innovation

Collaboration Analytics & Innovation must:

- Ensure that Information Assets enter and exit The City in compliance with the Access and Sharing Standard.
- Collaborate with internal Authorized Users to ensure that Data is made available through the proper self-service portal (e.g., Open Data or City Online)

INFORMATION SECURITY CLASSIFICATION

The City uses the following three information security classifications:

Classification	Unrestricted	Confidential	Restricted
Definition	Information that is unlikely to cause harm to individuals or to The City if released publicly This is the default classification.	Information that is valuable or sensitive to The City or requires protection by law, regulation, agreement, or City policy. This includes non-public, Personal Information that, if mishandled, could cause financial or reputational harm to The City or an individual.	• Information that is of high value or sensitivity, that if compromised, could put The City at financial or legal risk. • Information that is required to be treated as Restricted by law, regulation, agreement, or City policy.
Risks of Unauthorized Distribution, Modification or Loss	• Little or no impact to reputation • Minimal inconvenience if not available • Minimal financial loss	• Loss of reputation or competitive advantage • Loss of confidence in a City program • Reduce the level of public trust in The City • Penalties for violating the FOIP Act • Loss of trade secrets or Intellectual Property • Loss of potential revenue • Damage to partnerships	• Significant loss of reputation or competitive advantage • Serious loss of confidence in a City program • Substantial reduction of the level of public trust in The City • Injury or loss of life • Extreme impact to public safety • Catastrophic financial loss • Catastrophic damage • Sabotage and terrorism

	Unrestricted	Confidential	Restricted
Examples	• Most internal correspondence • Published Council Meeting Minutes & Agendas • White papers • Most meeting minutes • Fee schedules • Building permit files • Public Health and Safety information • Job titles, job descriptions, pay scales • Information received from partners or government that is freely available in the public domain	• Employee usernames, employee identification numbers and passwords • Personal or financial Information related to individual citizens or businesses • Highly valued Intellectual Property • Material prepared for in-camera Council meetings • Material subject to legal privilege • Testing and auditing procedures • Negotiation Information related to suppliers and third parties • Contracts	• Architectural plans for sensitive facilities and critical infrastructure • Security procedures • Items of high political or legal sensitivity • Information which The City is required to classify and protect as Restricted by law, contract, or agreement • Where the potential loss from unauthorized disclosure, alteration or unavailability of Information is expensive
Multi-class Information	If the Information System or Information Asset contains sections with different information security classifications, reasonable efforts must be made to separate out and/or make available the Unrestricted portions. If the sections cannot be separated, then the highest level of classification and protection must be applied to ALL the Information.		

If there is any ambiguity between two levels with respect to classification, the Information must be classified at the higher level until it can be definitively classified.

INFORMATION ASSET PROTECTION REQUIREMENTS

Information Assets must be protected in accordance with their information security classification.

The minimum protection requirements necessary at each security classification level are specified in appendices to this Standard.

- Appendix A: Storing City Information
- Appendix B: Communication of City Information
- Appendix C: Labelling of City Information
- Appendix D: Disposal of City Information

The appendices will be updated as required due to technology changes, availability of new controls, and changes to the threat landscape.

Information assets must be managed throughout their lifecycle (creation, use, retention and disposal), according to the Records Management Administration Policy and the Corporate Records Management Program.

Appendix A: Storing City Information

	Unrestricted	Confidential	Restricted
Hard Copy Information			
	No security-specific storage requirements	Must be locked in an office, desk or filing cabinet when unattended	Must always be attended or physically secured e.g. Locked in a secure filing cabinet or secure room
Electronic Information – Original and Authoritative Versions			
	Original and authoritative versions of all City information must be stored on City-managed storage.		
Network Drives (available on the corporate network, e.g. H:, S: drives)	Allowed	Allowed with appropriate access restrictions in place. Encryption recommended.*	Allowed with appropriate access restrictions in place. Encryption required.*
Content Server	Allowed	Allowed with appropriate access restrictions in place. Encryption recommended.*	Allowed with appropriate access restrictions in place. Encryption required.*
City-managed Cloud Services (e.g. OneDrive)	Allowed	Allowed. Information is encrypted by default.	Not Allowed
City-managed Cloud-based Collaboration Platforms (e.g. Microsoft Teams)	Allowed	Allowed. Information is encrypted by default.	Not Allowed
Other Cloud Services	Third party services may only be used when approved by Corporate Cloud Computing Stakeholders Team		Not Allowed
* Consult with Corporate Security and IT.			

	Unrestricted	Confidential	Restricted
Electronic Information – Temporary Copies			
	- Temporary copies of City Information for sharing or for offline use following an approved business process may be stored only as described below. - If the business process requires that changes to a temporary copy be reflected in the original version, appropriate measures must be taken when copying or synchronizing with the original Information to ensure the Integrity of the Information is maintained.		
Storage of a copy on City-managed Device (e.g. C: drive of a laptop or PC, iPhones, iPads)	Allowed	Allowed Information is encrypted by default.	Not allowed
Storage of a copy on removable media (e.g. USB stick, CD, DVD, external disk drive)	Allowed	Not allowed	Not allowed

Electronic Information – Non-Employees	
	Contractors, consultants, and other non-employees must use only City-managed devices, platforms, or cloud services to process or store City Information unless this is explicitly permitted by the terms of their contract or approved in writing by their City contract manager. The Information concerned must be appropriate to the provisions of that contract.

	Unrestricted	Confidential	Restricted
Electronic Information – Access Control and Audit Logs			
Access Controls	No special procedures. May be required for business purposes.	• Use of role-based access controls required • Access via City network or VPN	• Use of role-based access controls required • Access via City network or VPN
Audit Logs	No special procedures. May be required for business purposes.	• Logging must be enabled and active for all systems • Audit logs must be promptly backed up and automatically analyzed • Anomalies identified must be reviewed by Corporate Security	

Care must be taken to protect the Integrity and Availability of Unrestricted Information published electronically to prevent unauthorized modification that could harm the reputation of The City.

For any cases not covered above, consult with Corporate Security.

Appendix B: Communication of City Information

	Unrestricted	Confidential	Restricted
Internal Sharing	Internal sharing of Information Assets is encouraged wherever possible and appropriate to further business activity and facilitate knowledge reuse. Internal sharing of Personal Information should be consistent with the purpose of its collection. Send requests to the appropriate Information Steward.		May only be shared on a strict need-to-know basis and only with a minimum number of explicitly named individuals.
External Sharing	Allowed	Requires a license agreement May require a Privacy Impact Assessment	Not allowed
	The above is general guidance only. Refer to the ***Access and Sharing Standard*** for details on internal and external sharing of City of Calgary Information Assets.		
Hard Copy Information			
Transfer (Mail, Courier, Internal Mail)	No special procedures	• Sealed confidential envelope • Use only a reputable company or a trusted employee.	• Tamper evident packaging (e.g., double-sealed envelope with inside envelope signed to reveal evidence of tampering) • Handled under a continuous chain of custody with receipts documenting everyone who obtained custody • Use only a reputable company or a trusted employee. • Only the inner envelope is to be labelled with "Restricted" • Consider enclosing an acknowledgement slip to be signed by the recipient, confirming understanding of Restricted precautions.
Electronic Information			
Transmission (e.g. SMTP (Email), SFTP, HTTPS)	No special procedures	• City-approved encryption must be used • Confidential Information contained in or attached to email must be encrypted • Consider including handling instructions for the recipient, including disposal instructions.	• Must never be transmitted in unencrypted form • Consult with Corporate Security prior to implementing encrypted transmission of Restricted Information • Include handling instructions for the recipient, including disposal instructions.

<table>
<tr><th></th><th>Unrestricted</th><th>Confidential</th><th>Restricted</th></tr>
<tr><td><b>Public conversations</b></td><td>Be cautious to limit discussion of City of Calgary business in public locations.</td><td colspan="2">Take care so that only those with a need to know can hear your conversation. Special care should be taken in discussing sensitive Information when traveling to or participating in meetings away from City of Calgary work sites.
Confidential or Restricted Information should be clearly identified as such to all participants in the conversation.</td></tr>
<tr><td rowspan="2"><b>Photocopying & Printing</b></td><td rowspan="2">No special procedures</td><td>Carried out or supervised by the originator, a trusted nominee, or a trusted service organization that has signed a non-disclosure agreement.</td><td>Carried out or supervised by the originator, a trusted nominee, or a trusted service organization that has signed a non-disclosure agreement. Each copy must be tracked and marked with a unique number. (e.g. 1 of 10, 2 of 10, etc.)</td></tr>
<tr><td colspan="2">Be aware that printers and photocopiers usually retain a copy of the document on internal storage (i.e. hard disk) until the space is required for other documents. (Possibly weeks or months, depending on usage.)</td></tr>
<tr><td><b>Faxes, receiving</b></td><td>No special procedures</td><td colspan="2">Consult with IT and Corporate Security.</td></tr>
<tr><td><b>Faxes, sending</b></td><td>Check that the correct fax number is dialed and that the cover sheet is correctly completed.</td><td>Because most fax machines can store messages, physical access to both the sending and receiving machine should be limited to authorized individuals.</td><td>Faxing Restricted Information is <b>very strongly discouraged</b>. Because most fax machines can store messages, physical access must be limited to authorized individuals.
Prior arrangements must be made with the recipient to ensure that the receiving machine is attended by a trusted nominee or secured in a locked cabinet or room.</td></tr>
</table>

	Unrestricted	Confidential	Restricted
City of Calgary internal telephone	Allowed	Allowed Consider the possibility of being overheard.	Safe for City office-to-office Restricted communication. Consider the possibility of being overheard.
Normal wired telephone lines (non-City of Calgary)	Allowed	Use caution and bear in mind that telephone lines may be intercepted. Avoid unnecessary mention of sensitive items.	Should not be used for Restricted communication. If use is unavoidable, use pre-arranged code words to avoid references to individuals, companies, and projects.
Voice Calls on City-managed cell phones & smartphones	Allowed	Avoid unnecessary mention of confidential items	Use for Restricted communication is very strongly discouraged. If use of cell phone is unavoidable then consider using pre-arranged code words for individuals, companies, projects, etc.
Text Messages on City-managed cell phones & smartphones	Allowed	Text messages can be intercepted. Sending numbers can be impersonated. Avoid unnecessary mention of confidential items	Use for Restricted communication is very strongly discouraged. If use of text messaging is unavoidable then consider using pre-arranged code words for individuals, companies, projects, etc.

	Unrestricted	Confidential	Restricted
Voicemail (City Internal and City Cellular)	Allowed	Confidential Information should be left only with caution. Consider extra precautions, e.g. an introductory message not to listen via speakerphone and a suggestion to delete the message.	Restricted Information must not be left in a voice mail message
Voicemail (Personal, Other Organizations)	Allowed	Not Allowed	Not Allowed
City-Managed Teleconference & Videoconference Systems (i.e. Microsoft Teams)	Allowed	Allowed	Consult with IT and Corporate Security.
Non-City-Managed Teleconference & Videoconference Systems (e.g. Zoom, WebEx, apps with video calling)	Allowed	Not Recommended If used, be confident of the identities of the participants before disclosing Confidential Information. Be aware that recordings can occur without notice to participants.	Not Allowed
Hotel telephones	Allowed	Not recommended. Hotel phones, including lobby/courtesy phones, are insecure.	Not Allowed
Public telephones	Allowed	Not recommended. May be easily overheard and operated with minimal security.	Not Allowed

	Unrestricted	Confidential	Restricted
Non-City-Managed Internet Voice Services **(e.g. Google Voice, WhatsApp, Snapchat, Messenger)**	Allowed	Not allowed	Not allowed
Outlook Calendar	Allowed	Confidential meeting details or attachments available through Outlook Calendar must be hidden from view by flagging the meeting as “Private”.	Do not include Restricted Information in the body or attachments to a calendar item. A link to an access-controlled location may be included.
		Caution: When a user’s calendar is shared, meeting agendas and distributed attachments are also viewable by those with access to the shared calendar.	
Internal meetings and conferences	Allowed	Hold meetings behind closed doors.	Hold meetings behind closed doors. Consider maintaining a secure room (kept locked when not in use) for regular meetings.
Presentations **(e.g. PowerPoint, flipcharts, printed media)**	Allowed	• Information displayed must not be viewable by unauthorized persons (e.g. open doors or outside windows). • All items should be clearly marked ‘ISC: Confidential’; this should also be displayed when projected for viewing • Ensure all Confidential Information is collected or destroyed afterwards.	• Information displayed must not be viewable by unauthorized persons (e.g. open doors or outside windows). • All items must be clearly marked ‘ISC: Restricted’; this should also be displayed when projected for viewing • Ensure all documents are collected or destroyed afterwards. • Remind participants of how to treat Restricted Information.

	Unrestricted	Confidential	Restricted
External meetings and conferences	Allowed	Do not disclose meeting to non-attendees.	Do not disclose meeting to non-attendees.
		Hold meetings behind closed doors. Discretion should be used in choosing a suitable location.	Hold meetings behind closed doors. Use caution in selecting a location. Advice should be sought from City of Calgary Corporate Security. Consider carrying out a search for eavesdropping devices.
		See Presentations: Ensure all Confidential information is collected or destroyed afterwards.	See Presentations: Ensure all Restricted information is collected or destroyed afterwards.

Appendix C: Labelling of City Information

	Unrestricted	Confidential	Restricted
Hard Copy Information			
Hard Copy Information	No special procedures. If unlabeled, the document is considered Unrestricted by default.	Include "ISC: Confidential" clearly on: • each page of the document. • file folder labels • boxes containing Confidential Information	Include "ISC: Restricted" clearly on: • each page of the document. • file folder labels • boxes containing Restricted Information. Serially number each copy (e.g. No. 2 of 8 copies). • Assign each copy number to a named individual.
Electronic Information			
Email	No special procedures. If unlabeled, the email is considered Unrestricted by default.	Include "Confidential" in the subject line of email to inform the recipient of its classification.	Include "Restricted" in the subject line of email to inform the recipient of its classification. Refer to Restricted email conditions in Appendix B.
Files/folder names	No requirements.	Electronic documents (files), folders and directories should not have "Confidential" within their names.	Electronic documents (files), folder and directories should not have "Restricted" within their names.
Databases and Business Applications	Identify classification of data in system/application metadata. All applications and databases housing Confidential or Restricted information must be secured and have appropriate protection.		
Other Electronic Information and Documents	Identify the classification in the document's metadata. If additional classification options are available as part of a document management system, they must be used.		
		Where possible, include "ISC: Confidential" clearly on each page of the document.	Where possible: • Include "ISC: Restricted" clearly on each page of the document. • Serially number each copy (e.g. No. 2 of 8 copies). • Assign each copy number to a named individual.

Appendix D: Disposal of City Information

For all Information, including Corporate Records, the following disposal methods must be used.

	Unrestricted	Confidential	Restricted
Hard Copy Information			
Paper documents	Throw out or recycle. Shredding should be considered for documents containing valuable or sensitive information even if it does not meet the criteria for a Confidential classification.	Crosscut shred, or place in a locked container that has been designated for Confidential document collection and disposal.	Crosscut shred, or place in a locked container that has been designated for Restricted document collection and disposal. Log disposal details.
	Contact Corporate Security for guidance on required shredder specifications.		
Electronic Information			
City-Managed Storage	Delete and empty the Recycle Bin (or equivalent depending on the device or system)	Same as Unrestricted. Confidential Information must be stored in an encrypted format, so it will be unreadable even if recovered.	Contact IT and Corporate Security for assistance
Cloud Services	Certificate of Destruction from cloud service provider is recommended.	Certificate of Destruction from cloud service provider is required.	
Devices containing electronic files **(e.g. City of Calgary PCs, Laptops, Servers, Phones, Tablets, Disk Drives, Removable Media)**	City of Calgary IT's processes must be used to ensure secure deletion of information and disposal of the device, if required. If returning a device to IT: • If possible, delete Confidential or Restricted files • Inform IT if the device contained or still contains Confidential or Restricted Information If redeploying within your business unit: • Contact IT for assistance in securely erasing any information on the device • Do not redeploy the device before it is securely erased. Reformatting the device's storage is not sufficient.		

RESOURCES

Refer to the Administration Policy Library for the following:

Information Management and Security Policy

Corporate Records Management Policies and Program

Protection of Privacy Policy

REVISION HISTORY

Review Date	Description
13-Dec-2022	Revised descriptions of Information Security Classification levels; expanded and reorganized Information Asset Protection Requirements; added definitions and roles & responsibilities
30-Jan-2018	New Information Security Classification Standard reviewed and approved by Information Management and Security Governance Committee.