

Data Governance and Management

Edmonton

What's the Difference Between Data and Information? Who Cares!

Sean Clovechok

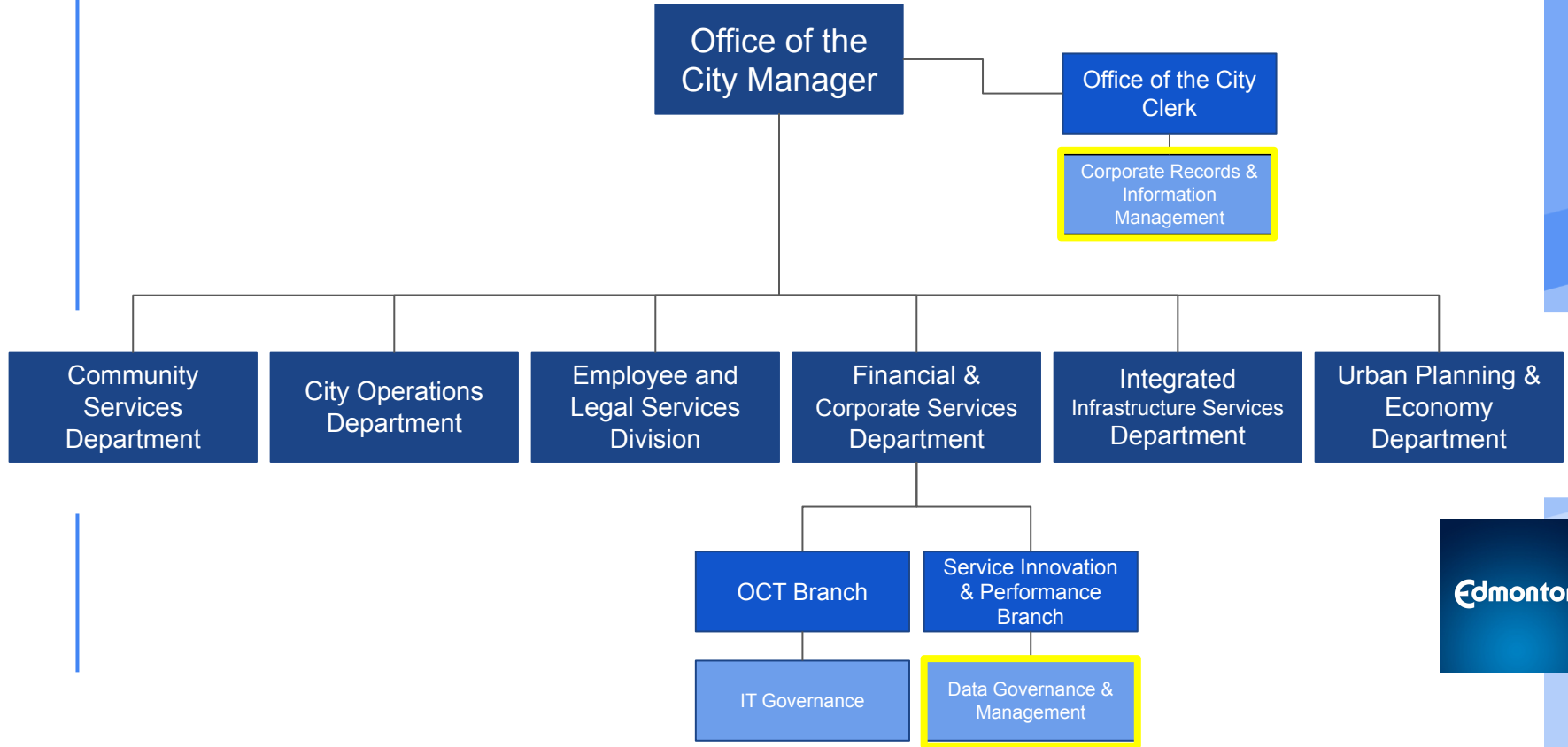
SIP

OCC

In the Beginning...

In a city called Edmonton there lived a municipal corporation. Not a backwards, archaic, messy corporation, filled with endless stacks of paper and strewn-about post-it notes, nor yet a perfectly organized, structured, data-centric corporation without a data management care in the world: it was a corporation that had evolved over time since 1904, and that means a lot of data.

There Was No Plan



Data Management vs Information Management ?



Data Governance Working Committee

- i. Archives
- ii. Business Solutions
- iii. Corporate Access and Privacy
- iv. Corporate Information Security Office
- v. Corporate Records and Information Management
- vi. Data Analytics
- vii. Data Ethics
- viii. Data Governance & Management
- ix. Data Science & Research
- x. Department (Business) Representatives
- xi. Branch (Business) Representative
- xii. Enterprise Performance Management
- xiii. Enterprise Commons (ERP upgrade)
- xiv. Geographic Information Systems
- xv. Legal Services
- xvi. Technology Planning & Business Engagement

Silo City

Seven attempts to
establish a corporate
body to oversee
information governance



Enterprise Commons

PeopleSoft

INTELEX

ORACLE®
Taleo X™

SAP
ECC

OPENTEXT
THE CONTENT EXPERTS

Daily Electronic
Time Entry
System

cority™



Edmonton

Data Governance Steering Committee

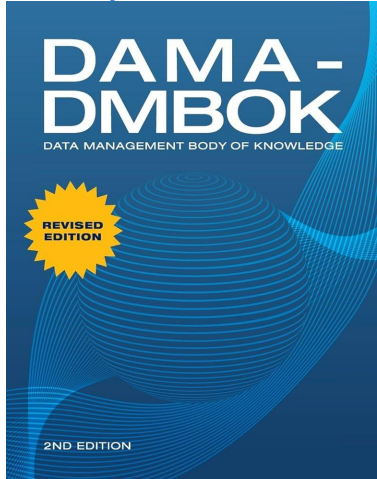
Branch Managers:

- **Service Innovation & Performance**
 - Data Analytics (BI)
 - Data Governance and Management
 - Data Science & Research
 - Geospatial Information Systems
- **Office of the City Clerk**
 - Corporate Access & Privacy
 - Corporate Records & Information Management
- **Open City & Technology**
 - Corporate Information Security Office
 - Other IT functions
- **Human Resources**
- **Financial Services**
- **Supply Chain Management**

Data Governance Steering Committee



Data and Information



"Both words of the DMBOK, data and information, will be used interchangeably."

High-Level Goals of Data and Information Management

- Accessibility
- Availability
- Compliance
- Informed Decision-making
- Lifecycle Management
- Privacy
- Quality
- Security
- Value Add
- Well Governed



Differences between DM and IM

- Data governance acts as the building blocks for the broader goals of information governance.



Policy

Tool	Purpose
Policy	WHAT - Sets strategy or provides direction to implement strategy
Procedure	HOW - Prescribes a process to achieve a policy's direction
Standard	HOW MUCH - Indicates a minimum level or quality for work
Guideline	OPTIONS - suggest a course of action

Administrative Policy Data and Information Management

Edmonton

Program Impacted	Project & Asset Management <i>The City of Edmonton's projects are well managed and assets are maintained for accountable service delivery.</i> Technology & Data <i>The City of Edmonton's technology and data are leveraged to enable quality decision-making and enhance innovative service delivery.</i>
Number	A1477
Date of Approval	July 13, 2023
Approval History	N/A

Policy Statement

As a data-informed organization, the City of Edmonton will manage its data and information assets as strategic resources in an integrated manner to maximize their value in use, both internally and externally.

The City will ensure its data and information are managed in compliance with the law. The City is responsible for aligning with best practices, using data and information ethically, safeguarding data and information from harm, and protecting individual privacy rights.

Data and Information Administrative Policy

- **One overarching Data and Information Administrative Policy**
 - to identify strategic guiding principles and create cohesion across functional domains
- **Benefits:**
 - A unified policy structure
 - A demonstration of the importance of all of functional domains
 - Improved understandability
 - Increased awareness

The Impact

- Open by default
- Managing the entire lifecycle
- Continually engaging stakeholders
- Ensuring an integrated approach

A City that creates, uses, shares, and protects data and information as a strategic assets for the benefit of Edmontonians.

- Establishing accountability and decision-making authorities
- Using forward-looking and iterative practices and technology
- Balancing current and future requirements
- Aligning functional domains

Administrative Policy

Data and Information Admin Policy

Functional Domains

Access

Architecture

Business Intelligence

Governance

Lifecycle Management

Privacy

Security

Procedures, Standards, Guidelines, other policy/non-policy tools, etc.

Freedom of Information Requests Guideline	Application Backup Standards	Analytical Tools Guidelines	Auditing Standard	Classification & Retention Schedule Standard	Data Obfuscation Standard	Access Control Standard
Routine Disclosure Guideline	Cloud & On-Premise Storage Guideline	Artificial Intelligence Guidelines	Data Governance Accountability Matrix	Data Archival Processes and Workflows	Privacy Procedure	Communications Security Standard
Role-based Permissions Guideline	Data Origination Processes and Workflows	Business Intelligence Procedure	Data Normalization and Cleansing Guidelines	Data Collection/Creation Procedure	Privacy Breach Standard	Compliance Standard
Access to Data and Information Standard	Data Modeling and Design Standard	Data Science Procedure	Data Quality Standard	Data Destruction Processes and Workflows	Protection of Mobile Sensitive Data Guideline	Cryptography Standard
	Information Technology Investment & Architecture Procedure	Data Warehousing Standard	Master Data Management Guideline	Data Usage Procedure	Release of Personal Information to a Law Enforcement Agency Procedure	Cyber Security Aspects of Business Continuity Management Standard
	Migration Standard	Predictive, Prescriptive, and Unstructured Analytics Standard	Metadata Standard	Information Disposition Procedure		Cyber Security Incident Management Standard
		Reporting Guidelines	Naming Standard	Offsite Storage Transfer and Retrieval Procedure		Cyber Security Procedure
		Visualization Guidelines	Open Data Standard	Physical Record-Keeping Procedure		Digital Asset Management Standard
			Reference Data Management Guideline	Unstructured Record-Keeping Procedure		Operations Security Standard
			Stewardship Framework(s)	Legal Holds: Preservation of Records Relating to Legal Action Procedure		Physical and Environmental Security Standard
						Supplier Relationships Standard
						System Acquisition, Development and Maintenance Standard

Legend	
Gold	Exists as a policy instrument
Blue	Exists (not as part of a policy)
Red	Does not exist but recommended

Data and Information Admin Policy

Access

Freedom of Information Requests Guideline

Routine Disclosure Guideline

Role-based Permissions Guideline

Access to Data and Information Standard

Architecture

Application Backup Standards

Cloud & On-Premise Storage Guideline

Data Origination Processes and Workflows

Data Modeling and Design Standard

Information Technology Investment & Architecture Procedure

Migration Standard

Business Intelligence

Analytical Tools Guidelines

Artificial Intelligence Guidelines

Business Intelligence Procedure

Data Science Procedure

Data Warehousing Standard

Predictive, Prescriptive, and Unstructured Analytics Standard

Reporting Guidelines

Visualization Guidelines

Governance

Auditing Standard

Data Governance Accountability Matrix

Data Normalization and Cleansing Guidelines

Data Quality Standard

Master Data Management Guideline

Metadata Standard

Naming Standard

Open Data Standard

Reference Data Management Guideline

Stewardship Framework(s)

Lifecycle Management

Classification & Retention Schedule Standard

Data Archival Processes and Workflows

Data Collection/Creation Procedure

Data Destruction Processes and Workflows

Data Usage Procedure

Information Disposition Procedure

Offsite Storage Transfer and Retrieval Procedure

Physical Record-Keeping Procedure

Unstructured Record-Keeping Procedure

Legal Holds: Preservation of Records Relating to Legal Action Procedure

Privacy

Data Obfuscation Standard

Privacy Procedure

Privacy Breach Standard

Protection of Mobile Sensitive Data Guideline

Release of Personal Information to a Law Enforcement Agency Procedure

Security

Access Control Standard

Communications Security Standard

Compliance Standard

Cryptography Standard

Cyber Security Aspects of Business Continuity Management Standard

Cyber Security Incident Management Standard

Cyber Security Procedure

Digital Asset Management Standard

Operations Security Standard

Physical and Environmental Security Standard

Supplier Relationships Standard



City Operations

Responsible for keeping Edmontonians working, moving and thriving every day. By leading in environmental stewardship, this department takes an integrated, innovative and... [read more](#)

Datasets Products

221

7

Items Activity

Intelix Incidents

city-operations
Intelix Incidents for Park

Intelix Inspection

city-operations
Intelix Inspections for Park

Intelix Inspections

Capital Project C

city-operations
Capital Project Cost Sum

CJ13

Parks and

iNovah Payment

city-operations
iNovah Payment Types a

Waste Management

1.4 Return of Digital Assets

Control: All employees and external party users must return all of the City digital assets in their possession upon termination of their employment, contract or agreement.

2. Digital Asset Security Classification

Objective: To ensure that Digital Assets receive an appropriate level of protection in accordance with their importance to the City.

2.1 Classification of Digital Assets

Control: Digital Assets must be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

There are four security classification levels to classify City of Edmonton digital information assets.

The classification level must be established based upon the potential risk (negative business impact) to the City's Health and Safety, Environmental, Compliance, Reputational, or Financial concerns due to the loss of confidentiality, integrity, or availability of information.

Information Classification	Definition	Examples
Public	Information that has been or could be published that if unintentionally disclosed, damaged, or lost would have a <i>minimal</i> negative business impact to the City.	Information on public websites, announcements, approved news releases, job postings, business contact information etc.
Internal	Information that if unintentionally disclosed, damaged, or lost could have a <i>moderate</i> negative business impact to the City.	Business data or information, planning documents, communications that do not contain proprietary information, draft requests for proposals etc.
Confidential	Information that if unintentionally disclosed, damaged, or lost could have a <i>significant</i> negative business impact to the City.	Time and labour Information, succession planning information, intellectual capital, unreleased financial records, personally identifying information etc.
Restricted	Information that if unintentionally disclosed, damaged, or lost could have a <i>severe</i> negative business impact to the City.	Executive Leadership Team deliberations and supporting documents, City Council "In Private" reports and agendas, information protected under statutory solicitor-client privilege, trade secrets, criminal records, criminal and security investigations etc.

restricted

dataset

restricted

dataset

restricted

dataset

internal

dataset

Source	Classification Levels							
	Public		Protected A		Protected B		Protected C	
Government of Alberta	Applies to data and information that, if compromised, will not result in injury to individuals, governments or to private sector institutions.		Applies to data and information that, if compromised, could cause injury to an individual, organization or government.		Applies to data and information that, if compromised, could cause serious injury to an individual, organization or government.		Applies to data and information that, if compromised, could cause extremely grave injury to an individual, organization or government.	
	Public		Internal		Confidential		Restricted	
ISO 27001	Everyone has access.		All employees have access.		Most employees have access.		Only Senior Management have access.	
	Public		Low Security		Medium Security		High Security	
York Region *see below for determination chart	Cleared for sharing to the public without restrictions on access or use.		Can be shared within the Region or registered partners (municipalities and conservation authorities).		For use only on a "need to know basis".		Controlled access of information specific to an individual or group.	
	Protected	Protected A	Protected B	Protected C	Classified	Confidential	Secret	Top Secret
Government of Canada	Applies to information or assets that, if compromised, could reasonably be expected to cause injury to a non-national interest—that is, an individual interest such as a person or an organization.	Applies to information or assets that, if compromised, could cause injury to an individual, organization or government.	Applies to information or assets that, if compromised, could cause serious injury to an individual, organization or government.	Applies to information or assets that, if compromised, could cause extremely grave injury to an individual, organization or government.	Applies to information or assets that, if compromised, could reasonably be expected to cause injury to the national interest, defence and maintenance of the social, political and economic stability of Canada.	Applies to information or assets that, if compromised, could cause injury to the national interest.	Applies to information or assets that, if compromised, could cause serious injury to the national interest.	Applies to information or assets that, if compromised, could cause exceptionally grave injury to the national interest.

	Public	Internal	Confidential	Restricted
Does the data/information contain in-camera council reports and agendas, information protected under legal privilege, trade secrets, criminal records, criminal and security investigations?				✓
Does the data/information contain financial or payment card details, such as SIN, credit card number, bank account number?				✓
Does the data/information include biometric details needed to open technology devices, such as face, voice, or fingerprint, or is it government issued identification containing a photograph or signature like driver's license or passport?				✓
Does the data/information contain personal identifiable details that are collected through consent form/process, such as name, address?			✓	
Was the information obtained with an agreement that specifies sharing or confidentiality limitations between the City and the other party? If you require clarification on any confidentiality question, contact Legal Services.		Option 1 Public → Internal → Confidential → Restricted →		Option2 Public Protected A Protected B Protected C
Does the information relate to employment with the City?			✓	
Does the data/information contain time and labour				

Impact and Implementation



Cyber Security Audit

Info Sec Class Levels

Public	
Internal	
Confidential	 
Restricted	  

Recommendation:
Classify all of the City's data

Management Response

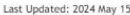
In order to comply with this recommendation, Administration will:

- Integrate and standardize data classifications 
- Apply new classifications to existing data sets

Implementation Date

~~New classifications: June 30, 2023;~~

Application: December 31, 2024



Function and Record Series

Purpose

The City of Edmonton Classification and Retention Schedule describes how we manage records and information at the City. It is a policy tool that classifies and assigns lifecycle management rules to all corporate records, regardless of medium or format.

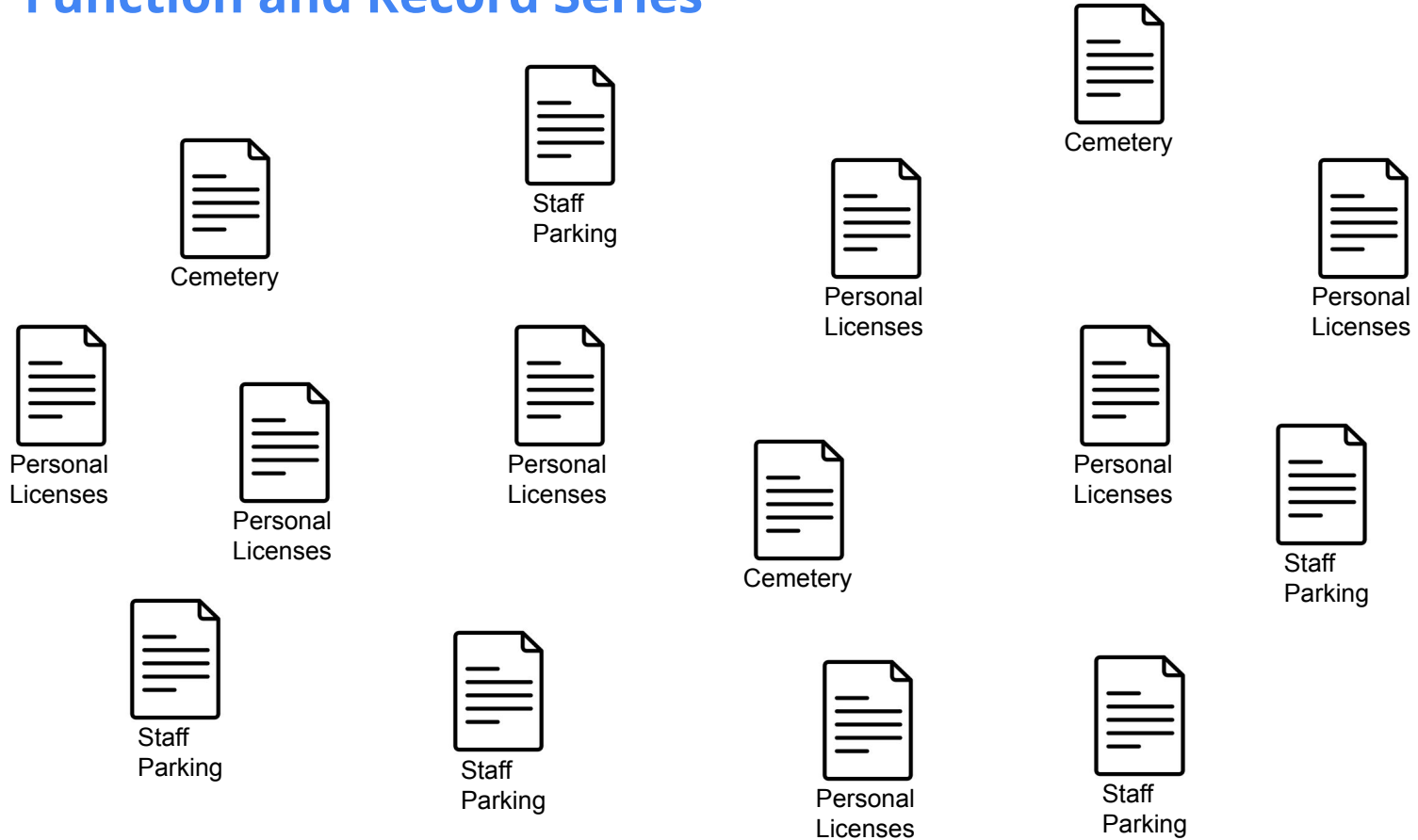
The City of Edmonton Classification and Retention Schedule allows the City to meet its operational, legal, technical, fiscal and historical information requirements. A standard classification and retention schedule facilitates:

- organizing related information into a common structure
- locating, accessing and using the correct information
- maintaining information for legislated time periods
- sharing information with the appropriate users
- reducing duplication and unnecessary storage costs
- minimizing loss of information, knowledge and corporate memory

The City of Edmonton Classification and Retention Schedule provides:

- descriptions of the records created, used and received at the City
- standards for how long the City must retain each record series
- notes on applicable legislation, corporate policies, industry guidelines, exclusions and procedural instructions

Function and Record Series



Function and Record Series

Retention Period

12 years



Personal
Licenses



Personal
Licenses



Personal
Licenses



Personal
Licenses



Personal
Licenses



Personal
Licenses



Personal
Licenses

Forever



Cemetery



Cemetery



Cemetery

2 years



Staff
Parking



Staff
Parking



Staff
Parking



Staff
Parking



Staff
Parking

Function and Record Series

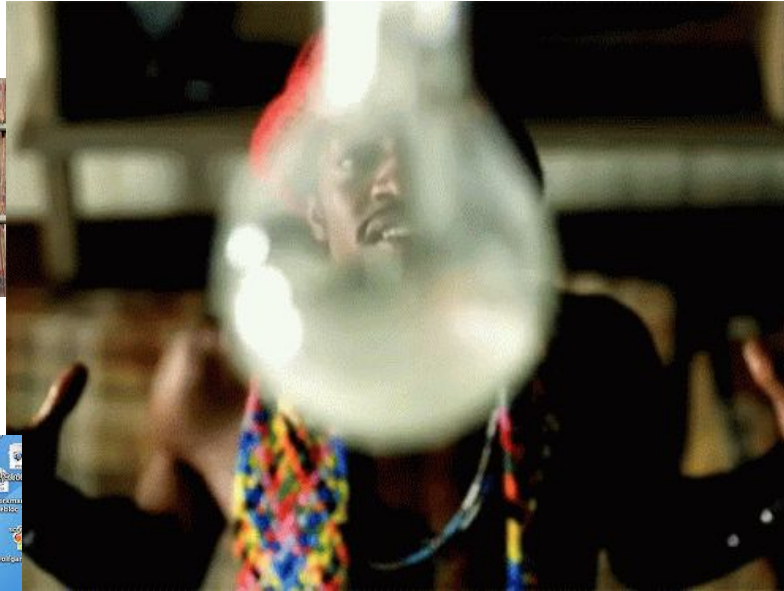


Using Classification and Retention Schedule to Satisfy Audit

Problem



Solution



Result



Edmonton

Mapping Info Sec Class to Record Series

010 Benefits, Payroll and Pension Programs

Information related to administering and managing programs offered by the Employee Services, including benefits, payroll, and pension.

Includes but not limited to:

- Administrative guidelines
- Automated time passing systems (e.g. generic systems information, history of decisions)
- Benefit programs procedures, reports, information for members (e.g. credit, life insurance, over-age dependents and pensioners programs)
- Change in benefit premiums
- Cheque distribution lists
- Procedures, guidelines and processing documents
- Program packages (e.g. sign-on, maternity leave and life changes)
- Reconciliations (e.g. medical, dental, travel, HCSA and life insurance)
- Reports (e.g. off-cycle, pension exceptions, affirmation letter, cost of living adjustment, mass retroactive payment)
- Sick or ill claim reporting (e.g. long term disability, sick, Workers' Compensation Board benefits)
- Termination of benefits reporting
- Union reviews

Retention

Trigger: Superseded or Obsolete

Period: 12 years

Based on: Business requirement

Disposition: Destruction

Systems: Google Drive: CRS HR Employee Service Centre

Core to: Human Resources

Security: **Restricted**

Excludes

- For individual employee benefit information, refer to *074 Benefit, Payroll and Pension Records*.

Notes

- n/a

2022 HUMAN RESOURCE MANAGEMENT

Mapping Info Sec Class to Record Series

Open Data Working Group

What

- Did initial mapping

Who

- CAP Office
- Data Analytics
- Legal Services

Data Governance Working Committee

What

- Validated Mapping

Who

- Data/Information SMEs
- Department Reps

Default Information Security Classification Reviewers

What

- Validated mapping

Who

- Branch Managers of the SME Branches

Initial Classification

064 Fire Services Permits and Inspections

Information related to issuing permits in accordance with the Fire Rescue Services Bylaw 15309, and the prevention and compliance inspections of buildings and properties. This includes transportation of hazardous materials permits, dangerous goods transportation permits, firework and pyrotechnic permits, fire performer indoor venue permits and open burning permits per municipal address.

Includes but not limited to:

- Applications
-
- Deficiency letters and reports
- Fire Code compliance
- Inspections and follow-up
- Letters to owners
- Orders
- Payment notice
- Permits
- Registration

Retention

Trigger: Cancelled, expired or refused

Period: 12 years

Based on: Limitations Act

Disposition: Destruction

Systems: POSSE

Core to: Fire Services

Excludes

Triggers for Classifying

ity classifications

- Use
- Manipulate
- Share

Followup Classification

Table 2: Conditions	Public	Internal	Confidential	Restricted
Does the data/information contain in-camera (i.e., private) council reports or agendas, information protected under legal privilege, trade secrets, criminal records, criminal or security investigations?			→	✓
Does the data/information contain financial or payment card details, such as SIN, credit card number, bank account number?			→	✓
Does the data/information include biometric details needed to open technology devices, such as face, voice or fingerprint, or is it government issued identification containing a photograph or signature like driver's license or passport?			→	✓
Does the data/information pertain to an investigation/litigation or the potential for litigation?			→	✓
Does the data/information contain business data or information, planning documents, communications that contain proprietary information, draft requests for proposals, etc.?			→	✓
Does the data/information contain personal identifiable details that are collected through consent form/process, such as name, address?		→	✓	
Was the data/information obtained with an agreement that specifies sharing or confidentiality limitations between the City and the other party? If		→	✓	

Applying Information Security Classification



Applying Information Security Classification

Info Sec Class

Restricted



Personal
Licenses



Personal
Licenses



Personal
Licenses



Personal
Licenses



Personal
Licenses



Personal
Licenses



Personal
Licenses

Confidential



Cemetery



Cemetery



Cemetery

Internal



Staff
Parking



Staff
Parking



Staff
Parking



Staff
Parking



Staff
Parking

Summary

- **Collaboration is everything**
- **More than just between DM & IM**
- **In the end, the differences don't matter**

“Alone we can do so little; together we can do so much.”



Thank You!

Questions?