RECORDS AND INFORMATION MANAGEMENT ACCOUNTABILITY POLICY

Department	Administration	Policy No.	0340-88
Section	Records and Information Management	Date Approved by Board	
Repeals		Board Resolution #	

Amended		Board Resolution #	
Amended		Board Resolution #	
Amended		Board Resolution #	

Repealed		Board Resolution #	

1. Purpose

1.1 The purpose of the Records and Information Management (RIM) Accountability Policy is to identify and formalize the roles and responsibilities within the Peace River Regional District (PRRD) for the management of PRRD's information assets. Every position has a role and a responsibility to manage information and records as corporate assets.

2. Scope

2.1 This policy, unless otherwise noted, applies to the PRRD Board members, employees, contractors and consultants.

3. Definitions

3.1 See RIM-01 Records and Information Management Framework Policy for definitions.

4. Policy

4.1 The following positions and groups are responsible for the listed functions and/or activities.

4.2 <u>Peace River Regional District Board</u>

PRRD Board members are accountable to:

- Ensure the implementation of a comprehensive Records Management (RM) program
- Approve and amend bylaws related to Records and Information Management and Freedom of Information (FOI) and Protection of Privacy which assigns responsibilities and authority to the Corporate Officer
- Provide the Corporate Officer with the resources necessary to perform the responsibilities required of the RM program
- Consider information security when working with PRRD records and information
- Immediately report any actual or potential information security incidents to the Corporate Records and Information Security Panel

- Immediately report any actual or potential litigation to the Corporate Officer

4.3 Corporate Officer

The Corporate Officer is responsible to:

- Approve and amend the Records and Information Management Policies and Procedures and the PRRD Records Classification and Retention Schedule (RCRS)
- Provide general oversight over the application of RIM Policies and Procedures
- Delegate RIM responsibilities and authority to the Corporate Services Coordinator
- Declare and manage the processes of a legal hold
- Approve all records destruction requests including destruction during a legal hold
- Resolve RIM issues that are elevated by the Corporate Services Coordinator
- Ensure that records are filed in accordance with the RIM policy and procedures
- Ensure that staff regularly identify and dispose of transitory and non-work-related records
- Work with the Corporate Records and Information Security Panel to respond to information security incidents and privacy breaches and identify opportunities to reduce the risk and likelihood of incidents and breaches
- Work with the Information Technology Manager to ensure proper security measures and best practices are in place to protect electronic information assets, with extra consideration of vital records, confidential and personal information
- Work with the Information Technology Manager to ensure that the systems managing PRRD's electronic records and information are reliable and secure; back up procedures are followed; electronic information assets are accessible, retrievable, and legible throughout their life cycle; and they are managed in a manner that ensures their integrity and authenticity

4.4 Corporate Services Coordinator

The Corporate Services Coordinator is responsible to:

- Implement the RIM program and delegate RIM program responsibilities to various positions and individuals as necessary
- Provide ad hoc and/or annual RM program reports to the Corporate Officer
- Manage the processes of records discovery or requests for records during litigation, with the input and advice of legal counsel
-
- Recommends regular file folder destruction and storage requests
- Develop and ensure compliance with the RIM policies and procedures
- Provide advice and guidance on RIM issues and topics
- Coordinate RIM projects
- Develop, maintain, update and ensure compliance with the PRRD RCRS
- Ensure the protection of vital records, with the assistance of the Information Technology Manager
- Ensure PRRD Board members and employees are trained on relevant RIM policies and practices

- Ensure forms comply with the PRRD's RIM policies and procedures, and the *Freedom of Information and Protection of Privacy Act*
- Create, organize and maintain PRRD filing structures according to the RCRS
- Develop, maintain, update and implement strategies for records conversions (e.g., scans or digital photographs) and records migrations (e.g., time resistant electronic formats and electronic system or repository transfers)
- Identify physical file folders that may be eligible for relocation to offsite storage
- Manage and track offsite and onsite file folder storage and act as the primary liaison with offsite storage facilities
- Identify file folders of all formats eligible for disposal and recommend and implement their disposal as per the approved retention schedule
- Create file folders according to PRRD standards
- Ensure the true deletion of electronic information assets identified for disposition according to the approved RCRS disposition schedules from all data repositories (excluding backup copies) in a timely fashion
- Work with the Corporate Records and Information Security Panel to respond to information security incidents and privacy breaches and identify opportunities to reduce the risk and likelihood of incidents and breaches
- Ensure a RM program compliance review is completed at least every five years and report results to the Corporate Officer

4.5 Department Heads

The Department Heads are responsible for:

- The administration and management of information assets in the department's custody
- Ensuring the department complies with the PRRD's RM program

4.6 Information Technology Manager

The Information Technology Manager is responsible to:

- Ensure that the information technology environment is compliant with the Regional District's RIM policies and procedures
- Implement access controls and permissions as defined by the Corporate Officer, in order to protect the PRRD's electronic information assets, with extra consideration of vital records and confidential or personal information
- Work with the Corporate Records and Information Security Panel to respond to information security incidents and privacy breaches and to identify opportunities to reduce the risk and likelihood of incidents and breaches
- Work with the Corporate Officer to ensure that the systems managing PRRD's electronic records and information are reliable and secure; back up procedures are followed; electronic information assets are accessible, retrievable, and legible throughout their life cycle; and they are managed in a manner that ensures their integrity and authenticity

- Assist in the true deletion of electronic information assets identified for disposition according to the approved RCRS disposition schedules from all data repositories (excluding backup copies) in a timely fashion

4.7 Employees

All PRRD Employees are responsible to:

- Ensure that records, including emails, are filed in accordance with the RIM policies and procedures
- Consider information security when working with PRRD records and information
- Immediately report any actual or potential information security incidents to the Corporate Records and Information Security Panel
- Immediately report any actual or potential litigation to the Corporate Officer
- Identify and regularly dispose of transitory and non-work-related records

4.8 Contractors and consultants

Contractors and consultants are responsible to:

- Provide any and all PRRD records upon request and/or at the end of a contract
- Consider information security when working with PRRD records and information
- Immediately report any actual or potential information security incidents to the Corporate Records and Information Security Panel
- Immediately report any actual or potential litigation to the Corporate Officer

Affiliated Policies	Records and Information Management Framework Policy 0340-87 Records and Information Management Policy 0340-89
Affiliated Procedure	Response to an Information Security Incident