Data & Information Management Policy

Owner: Chief Data Officer

Effective date: May 25, 2012
Last updated: May 17, 2021
Last reviewed: November 3, 2023

Data and information, including knowledge and intellectual property, is a valuable corporate asset that is integral to the company's business activities. Cenovus is committed to ensuring that the management and protection of its information and data meets business, legal, contractual and regulatory requirements through defined accountabilities, controls and processes as set out in this Policy and related standards.

Purpose

The Data & Information Management Policy (Policy) establishes a governance framework to achieve efficient, effective and secure management of Cenovus's data and information in support of business objectives, informed decision-making and a trusted reputation.

Cenovus encourages and promotes the use of data and information to leverage its value while managing the associated risks. Cenovus is committed to integrating good data and information management practices and capabilities into our business processes through appropriate governance and technologies.

Scope

This Policy covers all Cenovus data and information, regardless of the location it is stored, its form or how it is accessed. It applies to Cenovus Energy Inc., its subsidiaries and affiliates, and all Cenovus staff.

Roles and responsibilities

Business functions are responsible for assessing the business needs related to the data and information within their areas of responsibility. Each business function is responsible for appropriate governance, business planning, implementation, management and support of their data and information programs, in compliance with enterprise requirements, in order to leverage data and information for trusted decision-making. Business functions are expected to work collaboratively with stakeholders including third-parties, contributors and consumers of their data and information.

The Corporate Data Office (CDO) is responsible for developing, communicating and implementing a company-wide data strategy that introduces data governance, capabilities, standards and guidelines to enhance data literacy and improve the enterprise usability of company data and information assets. The CDO partners with business functions to facilitate access, improve quality and trustworthiness throughout the data and information lifecycle.

Information Technology (IT) is accountable for managing, supporting and protecting the systems and applications used to create, store, transmit and access information, including identifying the security requirements necessary to protect information, ensure its integrity and managing incident response and recovery. IT is responsible for the technology strategy and architecture required to meet business, statutory and regulatory requirements.

Records Management (RM) is responsible for providing guidance on the management of data and information through its lifecycle, from creation to destruction, with the goal of ensuring the principles contained within this policy are adhered to.

Staff are responsible for the management of data and information acquired or created in business activities conducted on behalf of the organization, in accordance with enterprise standards and processes. Cenovus expects staff to appropriately utilize and share the data and information that's created or captured for the benefit of the organization, and to reflect the relevant behaviours as required by the Code of Business Conduct & Ethics.

Policy statements

Ownership and value

- Subject to applicable regulatory and legal obligations, data and information acquired or developed by or for Cenovus is owned by Cenovus and is integral to Cenovus's success.
- The resources and effort expended on the creation and management of Cenovus's data and information is commensurate with the risk and value of its related business activities.
- Business functions are the designated owner of the data and information created or captured by the business processes in their areas of responsibility.
- Intellectual property rights and proper use of data and information systems is understood and respected in accordance with Cenovus's Intellectual Property Standard.

Creation and capture

Data and information is created or captured:

- In support of business strategies, priorities and activities.
- Completely and in a consistent and efficient manner to provide an accurate reflection of assets, liabilities and business activities.
- For functional use and is reused wherever possible.

Access and use

Data and information is:

- Managed to enable consumption by technologies and business processes.
- Verified for quality according to the risk and value of its usage.
- Easily accessible as governed by Cenovus's Records & Information Management Standard.
- Available for use by staff according to their role, subject to regulatory, legal, privacy, policy or other restrictions.

Security and protection

Data and information is:

- Safeguarded from unauthorized access, unauthorized disclosure, use or destruction through appropriate security and access controls.
- Created, captured, handled, protected and disclosed according to its information security classification in Cenovus's Information Security Classification Standard.
- Used for reasonable and acceptable purposes that ensures its confidentiality, integrity and availability.

Sharing and collaboration

Data and information is:

- Used for collaboration and knowledge-sharing purposes in order to increase its value and trustworthiness.
- Made available cross-functionally, where authorized by the designated owner, to leverage its use beyond its original purpose.
- Mined from trusted sources for accurate decision-making, analytics and visualization.

Storage and retention

Data and information is stored:

- Appropriately to meet legal and business requirements.
- For a specific period of time as defined by Cenovus's Retention Schedule.
- In a manner that maximizes efficiencies without impeding business access.
- In systems which enable collaboration and lifecycle management.
- In Cenovus-approved and managed systems and software.

Privacy and confidentiality

- The collection, use and disclosure of personal information is in accordance with Cenovus's Privacy Policy, Staff Personal Data Privacy Standard and legal requirements.
- Data and information used under confidentiality or license agreements is handled in accordance with the terms of the agreement.

Disposition and destruction

- Data and information is disposed upon expiry of the retention period as defined in Cenovus's Retention Schedule.
- Disposition of relevant and material information is suspended upon legal notification.

Compliance and enforcement

Monitoring

Cenovus reserves the right to monitor, review, access and disclose its information, and the systems used to support it, for business, security, investigative, monitoring or legal purposes.

Misuse or mismanagement of Cenovus data or information should be reported to your supervisor, a Human Resources Business Partner, the Integrity Helpline or the Investigations Committee.

Consequences of non-compliance

Actions in violation of this Policy may lead to disciplinary action up to and including termination of employment or service arrangements. In cases where local or international law or regulations are violated, Cenovus has a responsibility to involve the relevant agencies.

Related policies and standards

- Acceptable Use of Information Technology Standard
- Artificial Intelligence Standard
- Data Management Standard
- Cloud Services Standard
- Electronic Messaging Standard
- Information Security Classification Standard
- Information Security Policy
- Intellectual Property Standard
- Mobile Computing Standard
- Privacy Policy
- Records & Information Management Standard
- Retention Schedule
- Staff Personal Data Privacy Standard
- Cenovus Risk Matrix

Glossary

Data: Individual facts stored digitally that can be retrieved to represent information and used to help make business decisions.

Information: Data that has been given value through analysis, interpretation or compilation in a meaningful form.

Trusted source: A centralized system or location which has been declared as the trusted repository for organizational data and information for purposes of business analytics, decision-making, or fulfilling business or regulatory needs.