Information Security Practice

Owner: Manager, Cyber Security

Effective date: July 25, 2014
Last updated: July 25, 2014
Last reviewed: August 30, 2017

Purpose

Cenovus staff members have access to and develop a great deal of information related to the Company and its business. In most cases, that information is the property of Cenovus or a related party (e.g. a joint-venture partner or vendor). In all cases, Cenovus staff must protect corporate information from unauthorized use, disclosure or access. Corporate information in any form – electronic, transmitted, printed and verbal – is a valuable corporate asset. This Information Security Practice establishes Cenovus's universal standards for protecting corporate information.

This includes practicing safe computing behaviours to reduce the overall occurrence of theft, loss, or misuse of Cenovus information assets. A breach in cyber security or loss of information assets can have serious consequences, depending on the sensitivity and value of the information and the extent of the breach.

The consequences can include:

- Unauthorized disclosure of confidential information
- Interruption or disruption in Cenovus's information services
- Financial losses related to correcting the situation
- Regulatory impact
- Legal actions
- Erosion of the shareholder and public trust in our organization

Scope

The goal of the Information Security Practice is to provide an environment that enables maximum, safe sharing of corporate information while maintaining the security of information and complying with the Records and Information Management Policy.

Roles and Responsibilities

Cenovus staff are personally responsible for protecting corporate information against unauthorized use, disclosure or access. That includes understanding and complying with this practice and any related policies, practices or standards, as well as reporting incidents involving unauthorized use, disclosure or access to corporate information.

Practice Statements

Information classification and confidentiality

- Unless otherwise classified, corporate information is to be treated as "Cenovus Internal," meaning it can be freely shared between Cenovus staff
- It is the responsibility of the individual who developed or provided the information to properly classify it and ensure it is handled appropriately
- All staff are responsible for preserving the confidentiality of corporate information they access, develop or provide

Information and information systems ownership

- Information developed by or for Cenovus is owned by Cenovus, unless otherwise defined by contracts or law
- Cenovus owns information systems (e.g. computers, paper files, audio or video recordings) in which corporate information is held

Digital Information access

- Cenovus staff are given access to corporate information systems (e.g. computer networks) through personal accounts
- Each staff member is assigned an account and is responsible for all activity that occurs under that account
- Staff must protect their accounts through the use of strong passwords and must not share their accounts or passwords or store this information in plain sight

Information systems protection

- Unauthorized connections to Cenovus information systems are prohibited
- Attempts to bypass, disable or defeat these controls will be considered a breach of policy
- Monitoring or tampering with Cenovus information systems, external sites or email messages is prohibited
- Only software purchased by Cenovus may be installed on company systems

Appropriate Use

- Staff must apply reasonable care and judgment in using electronic messaging and the internet during the course of their work for Cenovus
- Policies and practices related to confidentiality, privacy and appropriate business conduct must be applied to electronic messaging use in the same manner as any other business communications
- Cenovus staff must be aware of and comply with intellectual property rights (e.g. copyrights, patent rights, trade secrets) according to the law and the Cenovus Intellectual Property Practice
- Staff may only use the information for which they have been given authority through their employment or engagement contracts and job requirements

Compliance and Enforcement

Monitoring

Cenovus monitors, logs and audits system activity and can trace actions back to individual accounts.

Cenovus holds the right to review, access, and disclose for security, investigative, maintenance and legal purposes, the contents of all information stored on or transmitted through its information systems.

Cenovus contracts independent audits and assessments of company information systems in co-operation with Cyber Security as part of a regular security review process.

Exemptions and Waivers

Deviations from this practice or any supporting practices or standards require signed waivers from Cyber Security. Waivers are granted on a temporary basis and require joint approval from Cyber Security and the relevant business unit leader.

Consequences of Non-compliance

Actions in violation of this practice or other related Cenovus policies, practices or standards may lead to disciplinary action up to and including termination of employment or service arrangements.

In cases where local or international law is violated, Cenovus has a responsibility to involve the relevant law enforcement agencies.

Support

Questions? Email us at: Information.security@cenovus.com

Related Policies/Standards

- Records and Information Management Policy
- Elevated Access Security Practice
- Corporate Network Practice