

Information Security Practice

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 another 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. 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 sensitive information and complying with the Information Management Policy.

Responsibilities

Every Cenovus staff member is 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 guidelines, as well as reporting incidents involving unauthorized use, disclosure or access to corporate information.

Information Classification and Confidentiality

Cenovus classifies corporate information to determine how that information should be kept secure. Unless otherwise classified, corporate information is to be treated as "Cenovus Internal," meaning it can be freely shared between Cenovus staff. If information is more or less sensitive than this, 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 members are responsible for preserving the confidentiality of any corporate information they access, develop or provide.

Information and Information Systems Ownership

Corporate information developed by or for Cenovus is owned by Cenovus, unless otherwise defined by contracts or law. The Company also owns information systems (e.g. computers, paper files, audio or video recordings) in which corporate information is held. As a result, 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.

Digital Information Access

Cenovus staff members are given access to corporate digital information systems (e.g. computer networks) through personal accounts. Cenovus monitors, logs and audits system activity and can trace actions back to individual 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.

Information Systems Protection

Cenovus protects its information systems through multiple security controls (e.g. firewalls, security cards, virus protection). All staff members are required to comply with security controls at all times. Unauthorized connections to Cenovus information systems are forbidden. Attempts to bypass, disable or defeat these controls will be considered a breach of policy. Monitoring or tampering with Company information systems, external sites or email messages is prohibited. Only software purchased by Cenovus may be installed on Company systems.

Cenovus contracts independent audits and assessments of Company information systems in cooperation with Information Security as part of a regular security review process.

Appropriate Use

Staff must apply reasonable care and judgment in using email 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 email 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. Staff may only use the information for which they have been given authority through their employment or engagement contracts and job requirements.

Waivers

Deviations from this practice require signed *waivers* from Information Security. Waivers are granted on a temporary basis and require joint approval from Information Security and the relevant business unit leader.

Violations

Violation of this practice and its associated guidelines may result in disciplinary actions that can include, among other actions, dismissal or legal action. Reports of violations of this practice will be forwarded to the appropriate business unit leader, Human Resources and Information Security. In cases where local or international law is violated, Cenovus has a responsibility to involve the relevant law enforcement agencies.