Acceptable Use of Information Technology Standard

Owner: Director, Information & Cyber Security

Effective date: February 20, 2020
Last updated: November 1, 2023
Last reviewed: June 28, 2024

Cenovus is committed to ensuring the safe and responsible use of its information technology to protect the company and its reputation from damaging behaviors and actions, whether deliberate or inadvertent.

Purpose

This Acceptable Use of Information Technology Standard (Standard) outlines Cenovus's requirements, restrictions and expectations with respect to the use of Cenovus information technology.

For the purpose of this Standard, "information technology" includes Cenovus's physical computing systems, resources as well as Cenovus's digital assets such as networks, computers, laptops, tablets, cell phones, audio/visual systems, printers/copiers, phones, conference phones, software, applications, workloads, email, mobile apps, cloud services, and data & information systems. Information technology may have artificial intelligence (AI) tools enabled, in accordance with the Cenovus Artificial Intelligence Standard

Scope

This Standard covers all Cenovus information technology, regardless of the location, its form or how it is accessed. It applies to Cenovus Energy Inc., its subsidiaries and affiliates who access or house our digital assets, and all Cenovus staff (employees, contractors and service providers). Suppliers are expected to develop policies and standards in alignment with the requirements of this Standard.

Roles and responsibilities

Data & Information Technology Team (D&IT) is responsible for managing, supporting, and protecting the systems and applications used to create, store, transmit and access information. They are responsible for the technology strategy and architecture required to meet Cenovus's policy and business requirements.

Information & Cyber Security is responsible for monitoring for compliance with this Standard, and training and awareness related to acceptable use of information technology, as well as supporting investigations through electronic discovery (eDiscovery) and digital forensics.

Business functions are responsible for developing business processes that comply with the requirements of this Standard.

Staff are responsible for protecting the confidentiality and integrity of our information technology and for exercising good judgment when using Cenovus information technology. Information technology may only be used as permitted by this Standard and related policies and standards. Staff are responsible for reporting illegal or unacceptable use of information technology, actual or suspected. Cenovus expects staff to protect Cenovus information (including information deemed confidential by agreement) and information technology against unauthorized use, disclosure or access in accordance with this Standard and the Code of Business Conduct & Ethics.

Standard statements

Cenovus staff must be aware that their use of Cenovus information technology could affect Cenovus and its reputation. Tampering with, or attempts to bypass, disable or defeat security controls, is strictly prohibited.

This Standard also extends to the use of personal devices while conducting company business, or while representing Cenovus in a business capacity.

Staff are expected to use information technology appropriately and for lawful purposes only, respect the privacy of others, and maintain the confidentiality, integrity and availability of information that may come to their attention in the course of their work.

In accordance with the Information Security Classification Standard, staff are expected to ensure that non-public data or documents (i.e. information labelled as Internal, Confidential or Restricted) are not exposed to unauthorized individuals at any time, including during and outside of working hours.

All staff are required to lock or log off their devices when leaving such systems unattended.

Information technology may be subject to licensing agreements and have limitations more stringent than what is allowed by this Standard. Users are responsible for understanding and following the higher standard.

Staff are expected to exercise good judgment and not access illegal or inappropriate content while using Cenovus information technology. Information technology resources are provided for business purposes in serving Cenovus's interests.

Cenovus may block certain sites or applications that it considers illegal or inappropriate or pose an unacceptable level of risk. Sites or applications that are not blocked for access or download may nonetheless be unacceptable, including without limitation, the dark web. Staff are encouraged to report inappropriate sites that could put Cenovus at risk.

Staff must not expressly or implicitly represent themselves as an authorized representative of the company when expressing personal statements, opinions, or beliefs. For more information on Cenovus's expectations with respect to social media please refer to the Social Media Standard.

Staff should not use their Cenovus email for non-business focused Internet communication (e.g. consumer websites) or any social media accounts.

Unacceptable use of information technology

Unacceptable use of information technology, whether personal or business, includes but is not limited to creating, accessing, transmitting, exchanging, or storing information that:

- Would expose the company or its technology resources to virus attacks, spyware, adware, malware, or hackers, or that could compromise the security of Cenovus systems.
- Attempts to prove security weaknesses or system bugs except for Information & Cyber Security or its delegates.
- Is considered promotional and unsolicited in nature such as chain letters, junk mail or other advertising materials.
- Conflicts with Cenovus's purpose and values and/or reputation, or that could damage Cenovus's image or reputation.

Unacceptable use applies to content that is illegal or inappropriate, but also extends to excessive use of non-business-related sites or applications, including but not limited to, gaming applications, streaming services, chat rooms, blogs, discussion rooms or social networking sites.

Personal use

Limited personal use of Cenovus information technology such as the network (i.e. internet), phones, printers, software, cloud services and email, is permitted on a reasonable basis. Personal use is considered reasonable if it is occasional, does not interfere with performance of job duties and complies with this Standard.

Storage of personal content on Cenovus information technology must be lawful, comply with Cenovus policies and standards, and is expected to be reasonable in content and volume. Storage of personal content on Cenovus information technology is allowed as a convenience and should be temporary. Staff should not have any expectation for the return of personal content following the conclusion of employment or engagement with Cenovus. Staff should have no expectation that personal content will be backed up or recoverable.

Cenovus information must not be stored on personal devices nor sent, transferred, or emailed to personal accounts.

Respectful workplace

Unacceptable use of information technology, whether personal or business, includes but is not limited to creating, accessing, transmitting, exchanging, or storing information that:

- Is offensive or pornographic (including messages, images, cartoons, or jokes).

Constitutes a comment, joke or slur about an individual or group including those related to protected grounds such as national origin or ancestry, citizenship status, colour, family status, race, ethnicity, religious beliefs, gender, age, physical or mental disability, genetic information, veteran status, uniformed service member status, gender identity, or sexual orientation.

- Is illegal, including fraud, defamation, harassment (including cyber bullying), stalking, terrorism, threats, identity theft, online gambling, spamming, intimidation or plagiarism/copyright infringement.
- Conflicts with or is in violation of Cenovus's policies and standards, including but not limited to the Code of Business Conduct & Ethics or the Workplace Violence & Harassment Prevention Standard.

Personal and confidential information

In using Cenovus information technology, staff are expected to comply with the requirements of Cenovus's Privacy Policy, Staff Personal Data Privacy Standard, Information Security Classification Standard and related standards.

Unless explicitly authorized by law or Cenovus, staff must not collect, access, use or disclose confidential or personal information of others (e.g. documents, voice recording, video recording, camera images, etc.). Encryption must be applied where possible.

Copyright and intellectual property

Staff are prohibited from violating the intellectual property rights of others, including copyright, patent, confidentiality, or other intellectual property rights. Unacceptable use includes but is not limited to:

- Installing non-licensed software on Cenovus information technology systems, even if for business use. Only software purchased by Cenovus may be installed on Cenovus information technology systems.
- Unauthorized downloading, copying and/or distribution of copyrighted or licensed materials, including posting protected information to Cenovus's intranet without properapproval. (e.g. downloading or sharing unlicensed data such as photos, per use licensed technical standard, etc.)
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management shall be consulted prior to export of any material that is in question.

Commercial or political materials

Commercial, advertising or political material may not be distributed using Cenovus information technology unless authorized by our Communications and Government Affairs teams. Under no circumstances is Cenovus information technology to be used for personal commercial gain.

Compliance and enforcement

Information & Cyber Security monitors compliance with this Standard, including the investigation of alleged misuse of information technology (and subsequent reporting and escalation) to ensure that Cenovus information technology is used lawfully and appropriately.

All data created and/or stored on Cenovus's systems is subject to logging and monitoring by Cenovus. Monitoring of data may only be conducted by named individuals upon authorization.

Information technology controls – monitoring, reviewing, accessing, retrieving, searching and/or disclosing – of content may be done so reasonably for authorized investigation, audit or legal purposes including for purposes related to the health, safety and security of staff and property; to ensure the efficient use of Cenovus's systems and equipment; to protect Cenovus property; and to ensure compliance with applicable laws and Cenovus policies.

Attempts to bypass, disable, tamper with, or defeat these controls is strictly prohibited.

Staff using Cenovus information technology, equipment, resources, property or accessing Cenovus information, systems or networks should not have any expectation of privacy with respect to their use of Cenovus information technology, systems, property or resources.

In cases where local or international law or regulations are violated, Cenovus may have a responsibility to inform relevant legal and/or regulatory authorities.

The requirements, restrictions and expectations in this Standard are by no means exhaustive but attempt to provide a framework for activities which demonstrate acceptable use. For situations not expressly addressed by this Standard, applicable rules and regulations may be referenced.

Exemptions and waivers

Deviations from this Standard require a waiver from the Information & Cyber Security team. Waivers are granted on a temporary basis following a risk assessment and require joint approval from Information & Cyber Security and the relevant business unit leader.

Consequences of non-compliance

Violation of this Standard may lead to disciplinary action up to and including termination of employment or service arrangements.

Support

Contact information.security@cenovus.com for questions related to this Standard.

Related policies and standards

- Credential Protection Standard
- Electronic Messaging Standard
- Elevated Access Security Standard
- Facility Access Standard
- Intellectual Property Standard
- Information Security Classification Standard
- Mobile Computing Standard
- Privacy Policy
- Social Media Standard
- Staff Personal Data Privacy Standard
- Workplace Violence & Harassment Prevention Standard
- Artificial Intelligence Standard
- Code of Business Conduct & Ethics
- CASL Compliance Protocol
- Cloud Services Standard

Glossary

Digital assets: identities, data, infrastructure and workloads (e.g. applications).