

Acceptable use of information systems practice

Purpose

The purpose of this practice is to outline the acceptable use of information system assets and information at Encana. Encana's Information System assets include any equipment or service provided by Encana that can be used for communication or to create, reproduce or distribute information. Examples include but are not limited to: desktop computers, laptops, shared drives, document management systems, email systems, instant messaging (IM) systems, internet connections, 'BlackBerry' or other PDAs, printers, plotters, fax machines, telephones and cell phones. This practice directly supports the Information Management Policy which helps ensure that Encana is successful in meeting all regulatory and compliance initiatives in the process of securing information and information assets while aligning with Encana's business strategies.

Scope

This practice applies to all individuals who have access to Encana's information system assets and information that are either owned, licensed or leased by Encana.

Practice statements

General use and ownership of information systems

- corporate information developed by or on Encana's behalf is owned by Encana, unless otherwise defined by contracts or law
- Encana information must be classified and protected in accordance with the Information Security Classification Practice
- information systems and information whether managed or hosted on Encana's behalf, is still considered the property of Encana and is bound by this practice, unless a contractual agreement indicates otherwise
- Encana's information system assets are to be used for business purposes; however reasonable personal use is permissible
- All information and communications created, transmitted or stored through Encana's information systems are considered Encana-owned information assets and may be monitored, reviewed, accessed and disclosed for security, investigative, maintenance and legal purposes by authorized individuals. There should be no expectation of privacy on these assets.
- Individuals with accounts will only access systems, applications, files and data to which they have been granted access. The ability to inadvertently read, execute, modify, delete or copy information does not imply permission to do so.
- only authorized individuals may post content or create the impression that they are representing, stating opinions, or otherwise making statements on behalf of Encana on social networking sites, blogs or other internet sites

- only approved and authorized devices may be connected to Encana's network
- individuals who are aware of any event which threatens the availability, integrity or confidentiality of Encana's information, or which breaches the [Information Management Policy](#), any of its associated practices or is contrary to local law, must immediately contact the [Information Security Team](#)
- all individuals must take appropriate care to protect Encana information, systems and related equipment within their custody or care from loss, damage or harm
- Encana reserves the right to monitor compliance of this practice

System and network activities

Encana's systems, network and application assets include but are not limited to computing devices such as desktop computers, laptops, tablets, servers, software applications and network devices which are wired and wireless such as: access points, network bridges, hubs, switches, routers, PBXs, IP phones, termination hardware, and all cabling/wiring behind "port sockets" in the wall.

General use and principles

- Encana provides and maintains its applications, systems and network infrastructure for the primary purpose of conducting its business
- Encana maintains a high level of security for applications, systems and network infrastructure, the internal network (LAN, WAN), connections to external networks (the internet, external partner networks) and independent networks (SCADA)
- unauthorized access to any of Encana's applications, system and network assets is strictly prohibited. For additional guidance please refer to Encana's [Corporate Network Practice](#)

Unacceptable use

The list below is by no means exhaustive. The following activities are considered unacceptable use of Encana's information systems:

- sharing your account password with others or allowing the use of your account by others
- circumventing user authentication or security of any user account or information system asset
- installing unauthorized software, hardware or changing system configuration settings, unless explicitly defined by your role and responsibility
- engaging in any activity with the intent to disrupt Encana's network or systems
- executing any form of network monitoring, port scanning or security scanning unless this activity is a part of the individual's normal job and is formally authorized

Digital communications and internet usage

Encana's digital communications utilize a variety of information system technologies to create, transmit or store corporate information which include but are not limited to email, internet, intranet, SmartPhones, BlackBerry, text messaging, instant messaging (e.g. blogs, discussion boards, AIM, Yahoo), telephone transmissions (e.g. mobile phone, land phone, IP phone, modem), fax transmissions and social media (e.g. Facebook, Twitter, LinkedIn)

General use and principles

- Encana provides and maintains its digital communication systems for the primary purpose of business communications
- Encana Confidential and Restricted information should be encrypted if sending by email and instant messaging systems
- Digital communications are a growing focus of litigation. Digital information is not easy to eliminate, and can be copied and forwarded with ease, and can be read by people other than the intended recipient — including other Encana staff or outsiders. Therefore, individuals should draft and transmit all digital communications with care, considering the content, how it may be interpreted, the intended recipients and the possibility of redirection, misdirection and redistribution. Features that allow sending to “all”, groups and distribution lists should be used with caution.
- Digital communication systems must be considered as communication tools, not storage mechanisms. Each individual is accountable for appropriately retaining corporate information that they create, transmit or store.
- casual correspondence is communication that has no administrative, legal, fiscal or archival requirements or enduring business value for retention should be deleted from information systems as soon as its purpose is served
- Encana filters digital communications channels such as email and instant messaging to protect against malware and prevent congestion and service disruptions
- when using Encana-owned digital communications systems for internal or external communications, all individuals must comply with the Information Security Practice for Canada or the U.S., Business Conduct and Ethics Practice, the Policy on Disclosure, Confidentiality and Employee Trading, the Employee Privacy Practice, the Social Media Practice and the Commercial Privacy Practice
- Encana backs up email systems solely for business resumption (disaster recovery) purposes. Backup restore functions are not available for individual digital communications.
- Encana limits the size and type of email messages and attachments that can be sent outside of the company and received from external email addresses
- individuals that receive emails or instant messages containing inappropriate content should report this to the Encana Service Desk promptly

Unacceptable use

Individuals are prohibited from using Encana's information systems to:

- conduct or attempt to conduct any illegal or unethical activity
- intentionally transmit fraudulent, harassing, offensive, threatening or discriminatory materials which include but are not limited to hate literature, obscene materials, materials which contravene human rights legislation, and any other material that could reasonably be interpreted as a form of sexual, ethnic, gender-related, and religious or workplace harassment, or that have the potential to adversely affect Encana's reputation
- intentionally retain or transmit, internally or externally:
 - obscene or sexually explicit messages, pictures, cartoons or jokes
 - personal commercial, advertising or political material
 - viruses/malware
- distribute or divulge Encana's, our clients', vendors', or third party's, confidential, personal, private or proprietary information without the appropriate authorization and consent
- put Encana at risk of violating copyrights, licensing requirements and contractual obligations by downloading, transmitting, reproducing, displaying or using software, information, music, images, documents and other intellectual property that are not either explicitly licensed for Encana's use or explicitly licensed for unrestricted commercial use
- automatically forward any digital communication to external sources or personal devices
- use peer-to-peer file sharing applications or services unless authorized
- use any remote storage facility not authorized by Encana
- install or use non Encana-issued audio or video playing software unless authorized
- misrepresent or replace another individual's identity

Exceptions

Deviations from this practice, based on business need, 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 leads.

Enforcement

Violation of this practice and its associated guidelines may result in disciplinary action up to and including termination of employment or services agreement and/or legal action. Reports of violations of this practice will be forwarded to the appropriate business unit lead, Human Resources and Information Security. In cases where local or international law is violated, Encana has a responsibility to involve the relevant law enforcement agencies.

146173