Information System General Usage Policy

Hierarchy Level: Policy	**Document Type:** Code	**Page:** 1 of 7
Owner: Executive Vice President - Administration	**Applies to:** Devon US	**Doc. ID:** 112845128
Last Revised: 2/7/2018	**Review Cycle:** Every 1 Year	**Implemented:** 10/1/2000

1. Purpose

The Information System General Usage Policy ("Policy") establishes appropriate uses of Devon's Information Systems. Devon provides secure Information Systems in accordance with the Information Security Policy. Inappropriate use of Information Systems unnecessarily exposes Devon to increased legal risk, the risk of computer viruses, and other risks that may compromise Devon's network systems and services.

2. Applicability

This Policy applies to all US employees and to all equipment owned or leased by Devon (irrespective of location). In addition, prior to granting any contractor or consultant access to Devon's Information Systems, the contractor or consultant must have previously entered into an approved contractual agreement with Devon.

3. Company Assistance/Exceptions

To displace any uncertainty regarding the proper use of Devon's Information Systems, employees should freely consult with their manager. In certain instances, it may be necessary for the manager to discuss a particular situation with senior management of Information Technology (IT) or with Devon's Executive Vice President and General Counsel.

When applying this Policy, it is important to note that certain activities or assignments within Devon require specific employees to perform tasks that may, at times, be partially or wholly contrary to certain provisions of this Policy. In those situations, employees are required to exercise sound judgment, utilize appropriate security measures where available, and adhere to other policies. At the conclusion of the aforementioned activities or assignments the general application of this policy will apply.

4. Policy Statement

In the course of employment with Devon, employees will have access to Devon Information Systems. Employees and contractors should use Devon's Information Systems for communication of Devon business information. Information Systems, including all messages and data transmitted, received or stored, are the property of Devon. Effective information management and security is a team effort involving the participation and support of every person who deals with Devon's information and Information Systems. It is the obligation of all Information Systems users to review this Policy and conduct their activities accordingly. All employees and contractors are responsible for ensuring information is protected from unauthorized modification, destruction, or disclosure, whether accidental or intentional.

4.1 General Information on System Use

All Information Systems, including computer equipment and Internet access, have been provided by Devon for business use. All use of Devon's Information Systems must comply with Devon's Code of Business Conduct and Ethics and other applicable policies.

Employees and contractors may use Devon's equipment for limited personal use. However, the use of Information Systems for charitable activities, political endeavors, private business purposes, or religious causes is prohibited. The aforementioned restrictions will not apply to any Devon sponsored political action committee or any other Devon-approved charitable or political activity or action conducted within the scope of an employee's job.

4.2 Unacceptable Use – System and Network Activities

The following activities are prohibited:

4.2.1 Uploading, posting, or otherwise distributing or facilitating distribution of any content, including text, communications, software, images, sounds, data, or other information that is unlawful, threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, tortious, or invasive of another's privacy. Content that contains nude, explicit, or graphic images, descriptions or accounts of sexual acts (including sexual language of a violent or threatening nature directed at another individual or group of individuals), or that otherwise violates Devon's Code of Business Conduct and Ethics or other Devon corporate policies is prohibited.

4.2.2 Violating any person's or company's rights protected by intellectual property laws, such as copyright, trade secret, patent, or other similar laws or regulations. Examples of prohibited activities include, but are not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Devon.

4.2.3 Unauthorized copying of copyrighted music and other copyrighted material, including but not limited to digitizing and distributing photographs from magazines, books, or other copyrighted sources.

4.2.4 Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Appropriate management should be consulted prior to the export of any material that is in question.

4.2.5 Deliberate introduction of malicious programs into Devon's network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.2.6 Attempting to "hack," "break-in," social engineer, or modify the security of Information Systems.

4.2.7 Making fraudulent offers of products, items, or services originating from any Devon account.

4.2.8 Making statements about warranty express or implied.

4.2.9 Effecting security breaches or disruptions of network communication. Examples include, but are not limited to accessing data the employee or contractor is not intended to receive, logging into a server or account the employee or contractor is not expressly authorized to access, and/or engaging any type of denial of service (DoS) or malicious activity, or other similar actions.

4.2.10 Port scanning or security scanning without prior notification to and approval from IT Security.

4.2.11 Executing any form of network monitoring that will intercept data not intended for a specific machine, device, or account.

4.2.12 Circumventing user authentication or security of any host, network, or account.

4.2.13 Sharing or utilizing the account credentials of another person.

4.2.14 Adding, removing, or modifying corporate Information Systems without prior consent from the IT Department.

4.3 Unacceptable Use – Messaging and Communication Activities

The following activities are prohibited:

4.3.1 Sending or distributing unsolicited messages, including junk mail or other advertising material, to individuals who did not specifically request such material (e-mail "spam").

4.3.2 Any form of harassment via e-mail, telephone, messaging, or other electronic medium, whether through language, frequency, or size of messages.

4.3.3 Unauthorized use or forging of e-mail header information.

4.3.4 Distributing or possessing inappropriate material including, but not limited to any nude, pornographic, racist, hate-crime, or violent written or visual content.

4.3.5 Distributing messages disruptive to normal business operations.

4.3.6 Knowingly sending or distributing messages that contain a computer virus or malicious software.

4.3.7 Forwarding or blind copying messages marked confidential, privileged, or proprietary, without the permission of the sender or authorized manager.

4.3.8 Creating or forwarding chain letters, Ponzi, or other pyramid schemes of any type.

4.3.9 Failing to delete messages once they no longer serve a valid business purpose. Messages or attachments with a retention classification or subject to a legal hold will be retained in accordance with Devon's Management of Records (MoR) Policy or instructions from the Legal Department.

4.3.10 Sending messages that relate or pertain to the potential liability of Devon by e-mail or transmitting them over the Internet/intranet unless transmitted securely to ensure the integrity, confidentiality, and privileged contents of the message. Such matters may include, but are not limited to environmental issues, pending or potential litigation, or employee personal information.

4.3.11 Sending or distributing Devon sensitive, financial, or employee/contractor data to any location for personal consumption or use. For example, e-mailing Devon data to an employee's/contractor's Hotmail, AOL, or GMAIL or similar account.

4.4 Use of Devon Company E-mail Address

4.4.1 Employees and contractors may not use their Devon e-mail address to sign-up for services that do not have a legitimate business purpose and prior approval has not been provided.

4.5 Password Sharing and Disclosure

4.5.1 Employees and contractors must not disclose their password(s) to any person at any time, except as may be permitted by this Policy.

4.6 Instant Messaging and Chat, Peer-2-Peer Communications

4.6.1 Only instant messenger applications approved by IT prior to the application's use and installation are permitted. Chatroom and Peer-to-Peer technologies are not permitted. (Examples include, but are not limited to: IRC, ICQ, Gnutella, BitTorrent, Kazaa, etc.)

4.7 Audio/Video Streaming

4.7.1 Non-business related audio/video streaming is not authorized. If there are specific requirements for non-business related audio streaming (example: radio reception is unavailable) please contact IT Services at digitalsecurity@dvn.com to discuss the requirements further.

4.8 Personal Information System Equipment

4.8.1 Devon information should not be stored on personal information system equipment and/or personal cloud computing services (e.g. Google Drive, Dropbox, Box, or non-Devon networks) unless prior approval is received. Personal information systems containing Devon information are subject to review by Devon and the information therein may be reviewed or provided to third parties pursuant to claims, litigation, investigations, or similar actions.

4.9 Personal Use of Computing Devices

4.9.1 Employees and contractors must participate in Devon's Mobility Opt-In Program if they want to use approved personal devices to access all Devon applications, corporate e-mail, calendar, and contact information. The use of personal devices must comply with Company policy and security controls and may subject the personal device to a search of both Company and personal information as part of the legal discovery process. Devon processes and security controls may change at any point in time due to evolving changes in technology and risk management practices Devon employs.

4.10 Social Network Usage

4.10.1 Unless authorized, Devon employees and contractors are prohibited from distributing or posting any Devon information that is deemed to be proprietary or confidential on any Internet forums, multi-media sources, chatrooms, blog sites, wikis, social networking sites (examples: Facebook, YouTube, Twitter, LinkedIn, etc.), or any similar site without prior authorization from the information owner or Corporate Communications. Any internet posting should not include Devon's logo unless permission is asked and previously granted. Devon employees or contractor internet postings must adhere to copyright, fair use, privacy, financial disclosure, and other applicable federal, state, and local laws.

4.11 Distribution of Company (Physical and Electronic) Data

4.11.1 Company sensitive, confidential or proprietary data, trade secrets, employee personal information, or financial data may not be distributed to employees or third parties that do not have a business need to know. Information relating to environmental issues, reserve or financial data, and pending or potential litigation are examples of data covered by this prohibition.

4.12 Licenses and Copyrights

4.12.1 All employees must adhere to software license agreements. All hardware and software products (including any electronic devices being integrated with corporate hardware) must be approved by Devon's IT Department. The IT Department reserves the right to uninstall and/or remove any unapproved hardware or software from Devon Energy equipment or the network without the consent of the employee.

4.13 Ownership of Information

4.13.1 All information used to conduct Devon business is the property of Devon and subject to this Policy. Ownership of the information means such information may be monitored, audited, reviewed, or provided to third parties or the government by Devon. This could include information, software, or any other intellectual property created by an employee's or contractor's personal use of Devon equipment.

4.14 Expectation of Privacy

4.14.1 There is no expectation of privacy on Devon Information Systems. Private passwords do not guarantee confidentiality. The use of passwords for the purpose of gaining access to Information Systems is done for the protection of Devon, not the employees. All communications and files are subject to monitoring by Devon whenever, in Devon's discretion, there is a business need to do so or in the course of periodic routine monitoring efforts. Devon reserves the right to audit any employee's activity on the network, including e-mail and Internet use, at any time without the consent of the employee.

4.15 Payment Card Industry Data Security Standard (PCI DSS) Compliance

4.15.1 Compliance with the PCI DSS is required of all Devon employees and contractors and departments that accept, process, transmit, or store payment credit cardholder information. Only Devon employees who are properly trained may accept and/or access cardholder information, devices, or systems which store or access cardholder information. Only PCI DSS compliant equipment, systems, and methods may be utilized to process, transmit, and/or store cardholder information. Each Devon employee who has access to cardholder information is responsible for protecting that information in accordance with the PCI DSS and Devon policy and procedures (PCI DSS Procedures) The events and circumstances of a suspected security breach which could negatively affect cardholder information or Devon's compliance with the PCI DSS must be immediately reported to IT Information Assurance. Vendors and service providers operating on Devon property who accept credit cards must execute a contract addendum that ensures their compliance with the PCI DSS. Non-Devon employees who act on Devon's behalf must also comply with the PCI DSS.

4.16 Cloud Computing Services

4.16.1 In order to ensure the ownership and protection of Devon's intellectual property, employees and departments that consider utilizing any cloud-based solution must work with Devon's Legal and IT departments to establish a contract that adheres to a well-defined risk assessment model prior to using any cloud-based solution. The risk assessment model will take into account state and federal regulations and laws in addition to providing a framework employees and departments can reference when going through the process of selecting an cloud based solution (e.g. taking into account data privacy, data security (both physical and electronic), contract termination, intellectual property protection, and infrastructure considerations).

4.17 Reporting of IT Security Matters

4.17.1 Employees or contractors who receive unusual messages and/or encounter IT security issues or other concerns pertaining to Information Systems should report these to the IT Service Center: Oklahoma City 405.228.8300.

4.18 LEGAL ISSUES

4.18.1 Under no circumstances are employees or contractors authorized to engage in any activity that is illegal under local, state, provincial, federal, or international law while utilizing Devon resources. Employees and contractors who are uncertain as to whether an activity is unlawful should consult Devon's Executive Vice President and General Counsel's office.

4.18.2 Additionally, in the event any portion of this Policy is inconsistent with any applicable local law or regulation, the inconsistent provision will be deemed void and the balance of the Policy will be modified to accommodate the deleted provision(s).

5. Consequences of Violation of Policy

Any violation of this Policy may result in disciplinary action, up to and including termination of employment.

6. Other Considerations

The Policy Owner will review this policy annually.

7. Definitions

Devon/Company	Devon Energy Corporation and each of its direct or indirect wholly-owned subsidiaries.
Including	As well as any form of the term will not be limiting or exclusive.
Information Systems	Includes, among other things, Devon's computers, systems, network and Internet equipment, software, data, telephones, mobile devices, voice mail, cloud service providers, and facsimile machines.
Payment Card Industry Data Security Standard	The security standard established by the banking industry for the protection of credit card data.
Records	Records are created, received, and maintained by an organization in the course of business. Records support business decisions, litigation, government, and regulatory reporting. Records may be stored on any electronic or non-electronic media (e.g., paper, video and/or audio tape, film, microfilm or microfiche, hard drive, disk, or other electronic storage device) and may be in any format (e.g., books, forms, memos, spreadsheets, e-mail, or drawings).