Policy No.:	AUP – v2.0
Effective Date:	August 16, 2004
Revision Date:	January 17, 2013
Revision No.:	1
Approval	jwv / mkb

Information Security and Electronic Communications Acceptable Use Policy (AUP)

1. INTRODUCTION

Southwestern Energy Company, ("SWN" or "Company") provides to, and authorizes the use of Electronic Communication Resources (also referred to as ECRs and as defined below) by directors, officers, employees, contractors, agents or business partners of the Company, its subsidiaries or affiliates and other authorized persons or entities ("Users") solely for the purpose of conducting Company business. The provision of Electronic Communications Resources by the Company and the Company's authorization of their use by Users are expressly subject to the terms and conditions of this Information Security and Electronic Communications Acceptable Use Policy ("Policy") which may be updated from time to time. Each User agrees to review this Policy periodically in order to keep up to date with any modifications. This Policy is further intended to notify Users of the business and information security risks that are inherent with the use of publicly accessible communication networks. Any questions concerning this Policy should be directed to the Chief Information Officer. Users should periodically refer to the Q&A forum for answers to commonly asked questions concerning this Policy and use of the Company's Electronic Communications Resources.

This Policy supplements, and should be read in conjunction with, the Company's Business Conduct Guidelines and other policies and procedures (collectively, the "Codes of Conduct").

2. REVISION HISTORY

DATE	REV. NO.	CHANGE	REFERENCE SECTION(S)

3. SCOPE, RESOURCES & PERSONS AFFECTED

Proper use of the Company's Electronic Communication Resources is an enterprise function. This Policy thus applies to Southwestern Energy Company and all of its subsidiaries and affiliates.

The terms "Electronic Communication Resources," "ECR" and "ECRs" refer to the computer systems and networks owned by any of the Company, its subsidiaries or affiliates as well as telephonic and mobile communication devices and Internet and facility access provided by any of the Company, its subsidiaries or affiliates. ECRs include, but are not limited to, host computers, file servers, application servers, communication servers and equipment, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, software, data files, all internal and external computer and communications networks, intranets, extranets, facsimile machines, telecopiers, e-mail systems, phone systems, office voice-mail systems, cellular/mobile phones, Personal Digital Assistants (PDAs), electronic paging devices, two-way or broadband radios, and electronic facility security systems.

The restrictions and obligations set forth in this Policy apply to all Users wherever they may be located.

4. POLICY

a. USE

The ECRs covered by this Policy are the exclusive property of the Company. The Company provides the Users with access to these resources to conduct and support its business. Infrequent and occasional reasonable use of ECRs for non-business purposes is permitted, provided that such use does not 1) involve any activity prohibited by or in violation of this Policy, the Codes of Conduct or any other Company policy, 2) interfere with work productivity, 3) deplete system resources for business purposes, or 4) in any way conflict with the Company's business interests. Users who utilize any of the ECRs for personal reasons do so at their own risk and the Company shall not be responsible or liable for the integrity of personal data including, but not limited to, loss, corruption, unauthorized access or public exposure of such data, or the erasing or destruction of such personal data by Company.

b. PRIVACY

Users are given access to the ECRs to enable them to perform their job responsibilities. As set forth in Section 4c. of this Policy, passwords and other security mechanisms are used to control access to the Company's information and are not intended to confer upon a User an expectation of an individual right of privacy with respect to any information or material created, stored, sent or received via an ECR. As set forth in Section 10 and without advance notice to the User, the Company may access, monitor, read, disclose, review, erase and destroy any information or material created, stored, sent or received on its computer systems, networks or through the use of e-mail, the Internet, and/or voice-mail.

As a condition of use, each User expressly waives any right of privacy with respect to any information or material such User creates, stores, sends or receives via an ECR,

and each User acknowledges that Company may at any time erase or destroy any such information or material. Each User also expressly acknowledges and accepts that Company may at any time restrict, limit or eliminate any aspect of an ECR's functionality to such User. Further, Users consent to allow the Company to access and review all materials Users create, store, send or receive on the computer or through the Internet, e-mail, voice-mail, or any other computer network. Users understand the Company may use human or automated means to monitor or limit use of its computer, e-mail, voice-mail and other network resources.

The Company reserves the right, to the extent permitted by applicable law, to record or listen to telephone and cellular/mobile voice communications at any time and from time to time for legitimate business reasons. Users are further advised that 1) incidental access to telephonic or mobile voice-mail stored on systems of the Company or the Company's communication service provider may occur in the normal course of system administration by those authorized to maintain those systems, and 2) the Company's communication service providers submit to the Company periodic billing records pertaining to all telephone calls, mobile calls, and pager messages made or received by the Users.

c. ACCESS SECURITY

Access to the Company's ECRs is controlled through individual accounts, passwords and other security mechanisms. Primary management team leaders are responsible for defining appropriate access levels for the Users within their areas and conveying that information to the Information Security team via the Company's Service Request process.

Each User is responsible for all activities conducted using their passwords and/or access mechanisms. Each User is therefore responsible for safeguarding and protecting his or her password and other access mechanism. Individual passwords are not to be printed, stored online or given to others, and further must adhere to the specific rules for password creation and protection set forth in Schedule AU-1 of this Policy. Further, all ECRs are to be safeguarded against loss, theft, damage, or unauthorized use. Users may "delegate" access to their electronically stored information if there is a legitimate business purpose for doing so provided that prior approval is obtained via the Company's Service Request process.

Any actual, suspected, or potential security breaches, including, but not limited to, any unauthorized access, use or disclosure of, or damage or loss to, the Company's ECRs and/or information are to be reported immediately to the Client Services Helpdesk and/or the Chief Information Officer.

d. INFORMATION SECURITY and RELIABILITY

Each User is responsible for ensuring that use of the Company's ECRs, such as the Internet, does not compromise the security of the Company's information and computer resources. Each User must take reasonable precautions to prevent 1) intruders from accessing the Company's network without authorization, and 2) introduction and spread of viruses.

In addition, each User is responsible for safeguarding Company confidential information and to further ensure proper Company representation. All Company confidential or proprietary information is to be electronically transmitted only by 1) conventional telephonic facsimile, or 2) by e-mail in encrypted form by a method approved and administered by BIS before being transmitted.

e. PROHIBITED CONDUCT

Using Company ECRs for any illegal, fraudulent, abusive, unethical or other "inappropriate" purpose is strictly prohibited. Some examples of use of ECRs that will subject Users to disciplinary action (and potentially discharge) include, but are not limited to:

- Violating any local, state, federal, or international law;
- Sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is sexually explicit, profane, obscene, indecent, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful;
- Gambling;
- Soliciting for individual personal gain or profit;
- Representing yourself as someone else;
- Representing personal opinions as those of the Company;
- Posting messages or responses on Internet messaging/bulletin boards related to the Company.
- Operating a personal business;
- Uploading or installing software;
- Copying, downloading, or disseminating information that is proprietary or confidential to the Company;
- Knowingly copying or using software or data in violation of any license agreement, copyright, or patent;

- Soliciting employees or other third parties for religious, charitable, or political causes not specifically authorized by the Company.

- Accessing or attempting to intercept another person's e-mail account or misrepresenting, obscuring or altering another User's identity in an e-mail;

- Accessing or attempting to access another person's electronically stored data without proper authorization; and

- Intentionally interfering with the normal operation of the Company's ECRs or using any of the Company's ECRs to deliberately harm or circumvent the security or operation of the computing systems and networks of others.

5. E-MAIL RETENTION AND STORAGE

It is the responsibility of each User to retain and manage e-mail in compliance with the Company Records Retention Policy.

E-mail systems are not intended for the archival storage of Company records. Any e-mail messages sent or received that no longer require action or do not constitute a master record are to be promptly deleted. E-mail messages and content are not to be permanently stored on local hard drives or removable storage media (CDs, floppies, etc.). Any data that is stored on a removable storage device should be transferred to a permanent storage location as soon as practical and deleted from the removable storage media as soon as this information transfer is completed.

6. USE OF NON-COMPANY E-MAIL, INSTANT MESSAGING, OR STORAGE SYSTEMS

Use of non-Company messaging systems compromises Company security and other controls and increases the risks of unauthorized use, viruses and malicious programs. Therefore, Users shall use only Company messaging systems for its business communications. Users shall not use non-Company web-based e-mail, instant messaging or data storage systems for Company business except as specifically authorized for Company business and approved by the Chief Information Officer.

7. USE OF NON-COMPANY ECRs

Users shall not use any non-Company devices or connections other than those approved in advance of their use by the Company via its Service Request process.

Once approved, Users may use privately-owned devices and connections to remotely access the Company's ECRs within the stated hours of Company computer network

operation. In each such case, the Company will provide initial access set-up instructions. The Company will not otherwise provide any technical set-up assistance or support of privately-owned devices or third-party communication service provider connections.

Unless approved in advance by the Company, the Company is not responsible for any expenses that Users may incur in deploying, maintaining or using privately-owned devices or connections, including costs of third-party Internet and Telecommunication service providers.

The Company is not responsible for any damage to or malfunction of any privately owned devices or connections.

8. INADVERTENT or UNINTENTIONAL MISUSE

Given the "open" unregulated nature of the Internet, it is possible that a prohibited activity or misuse of the Company's ECRs could unintentionally occur. For example, an inappropriate web site may be accidentally accessed no matter how much care is reasonably exercised. Further, "spam" e-mail or e-mail from an outside source containing inappropriate content may be received even though preventative screening measures are taken. Users are encouraged to immediately report such incidents to the Client Service Helpdesk without any concern or threat of incurring the sanctions described in below Section 10. Users should also refer to the Company's SWNet for additional information on handling these situations.

9. RESPONSIBILITIES

All Company representatives, whether directors, officers, employees, contractors, agents, business partners, or any other Users, have a responsibility to safeguard Company information assets and to ensure that the Company's ECRs are used responsibly, professionally, ethically, and lawfully. To that end, all Users have the duty to understand and to comply with this Policy and the Company's other Codes of Conduct.

Primary management team leaders are responsible for 1) reviewing and either approving or disapproving User access to the Company's ECRs via the Service Request process, and 2) helping to ensure that their team upholds the provisions of this Policy and its intended purpose.

The Company's Chief Information Officer has accountability for interpreting this Policy, approving exceptions, and recommending any changes to Executive Management.

10. COMPLIANCE

Consistent with the Company's Business Conduct Guidelines, all violations of this Policy, except for Inadvertent or Unintentional Misuse as described in Section 8 above, are to be promptly reported to the Company's Corporate Compliance Officer. All violations of this Policy will be taken seriously and may result in 1) disciplinary action, including suspension or termination, and/or 2) civil or criminal liability. To ensure compliance with this Policy, the Company will routinely monitor the use, frequency, content (including intended addressees) and volume of all traffic utilizing the Company's ECRs.