


TransCanada Policies and Procedures		
Title Information Security Policy		
Effective Date (Date of Last Revision): 10/5/2011 Original Execution Date: 10/05/2011	UNCONTROLLED IF PRINTED Status: Approved	


This Policy applies to all Personnel (including full-time and part-time employees, contract workers, contractors and consultants) of TransCanada Corporation and its wholly-owned subsidiaries, and operated entities in Canada, the United States and Mexico (the "Company"). When appropriate, the policy will be included as part of contractual agreements with third-party stakeholders, such as customers and suppliers, that may access or create Company information systems and technologies.

This policy applies to all information systems and technologies maintained by and under the control of the Company. For the purposes of this policy this includes, but is not limited to:

- Company-related information,
- Computers, related systems including all data and programs,
- E-mail, voice mail, and other voice and data communication systems managed by the Company or a third party,
- Industrial control systems (SCADA) including Distributed Control Systems (DCS),
- Hand-held devices and personal communication devices (e.g. cell phones, smart phones),
- Company and external information storage facilities, where information resources are stored or managed via electronic or digital media or devices.

POLICY STATEMENTS

1. All information systems and technologies must be developed and maintained in a secure manner at all times.
2. All information and data must be maintained and secured in a manner consistent with the "Information Management Policy."
3. All information systems and technologies developed or acquired by or for the Company are property of the Company and must be used for Company approved purposes.
4. It is the responsibility of all department personnel to manage and secure their information systems and technologies (using tools and protocols supplied by Information Services).
5. Senior Leadership will be accountable to ensure information systems and technologies within their functional area are identified and assigned an Information Asset Owner (i.e. leader, manager).
6. Use of the Company's information systems and technologies must comply with all applicable corporate governance documents and all applicable statutory, legislative, regulatory, contractual, industry and operational requirements.
7. Information systems and technologies must be appropriately protected, from unauthorized or inappropriate access, use and destruction or disclosure whether accidental or intentional, throughout the systems lifecycle.
8. Information must be transmitted in a secure manner (e.g. encrypted, etc.), appropriate for its sensitivity, regardless of the media or communication method used.
9. All sensitive and valuable information systems and technologies must be appropriately secured when left unattended.
10. Incidents related to information security must be reported to IS Governance and Security, Business Information, Internal Audit, Human Resources, Legal, Corporate Security, Privacy Officer or others as governed by their respective corporate policies.

TransCanada Policies and Procedures		
Title Information Security Policy		
Effective Date (Date of Last Revision): 10/5/2011 Original Execution Date: 10/05/2011	UNCONTROLLED IF PRINTED Status: Approved	

COMPLIANCE / EXCEPTIONS

Personnel are expected to comply with all aspects of this policy and to support others in doing so. Personnel who fail to comply with a TransCanada Policy or its intent or who knowingly permit personnel under his or her supervision to not comply will be subject to disciplinary action up to and including termination of employment, termination of contract or removal from the Company's worksite. Please refer to the [TransCanada Policies and Procedures Web Site](#) for more information.

RESPONSIBILITIES

As owners of the Information Security Policy, Information Services mandate is to govern the security of the Company's information systems and technologies. The related responsibilities are as follows:

Information Services

- Provide training and awareness regarding the Information Security policy and standards.
- Track and resolve issues, concerns and incidents relating to the Information Security policy.
- Develop the IS security strategy, practices, standards and guidelines in support of this and other Company policies.
- Provide IT risk assessment and consultation services to support the Information Asset Owner, the Custodian and the personnel in the performance of their security of information responsibilities.
- The Vice President of Information Services is accountable to ensure that technology policies, standards, guidelines, tools, and processes exist to enable the protection of the Company's electronic information systems and technologies.
- The Vice President of Information Services is the Information Asset Owner of the IT Infrastructure.

Senior Management


- Ensure information systems and technology within their functional area are secured and personnel are held accountable for following this corporate policy.

Information Asset Owner

- Ensure all levels of access to information systems and technologies are aligned with business and regulatory requirements.
- Establish control over their information systems and technologies that meets all legal, regulatory and operational compliance requirements.

All Personnel

- Become informed about the Company's Information Security policy and maintain their information systems and technologies accordingly.

TransCanada Policies and Procedures		
Title <u>Information Security Policy</u>		
Effective Date (Date of Last Revision): 10/5/2011 Original Execution Date: 10/05/2011	UNCONTROLLED IF PRINTED Status: Approved	

REFERENCES AND LINKS

- [Questions and Comments](#)
- [Code of Business Ethics](#)
- [Information Management Policy](#)
- [Information Management Program](#)
- [Protection of Personal Information Policy](#)
- [NERC-CIP Cyber Security Program](#)
- [Acceptable Usage of Electronic Information Resources](#)
- [Corporate Password Standard](#)

Document Originator(s) Terry Lamb IS Governance and Security	Signature
Document Reviewer(s) Darryl Williams Director, IS Governance and Security Rick Coutts VP, Information Services	Signature
Approval(s) for Issuance Sean McMaster Chair, Corporate Performance Committee Executive Vice President, Corporate and General Counsel On behalf of the Committee	Signature