

Policy.



Acceptable Use Policy.

Purpose and scope

The purpose of this Policy is to describe the Company's expectations and requirements regarding the responsible, safe, reliable, and confidential use of TC Energy's Digital Assets, Digital Information and Accounts.

This Policy applies to all Personnel and Excluded Contractors in Canada, the U.S. and Mexico who use TC Energy's Digital Assets, Digital Information or Accounts for Company Business.

Policy

1 General provisions

- 1.1 Personnel and Excluded Contractors must use Digital Assets, Digital Information and Accounts in compliance with all applicable legal requirements and TC Energy's Code of Business Ethics (COBE) Policy, Data and Information Policy, Protection of Personal Information Policy, and the Inter-Affiliate Codes.
- 1.2 Personnel and Excluded Contractors must use TC Energy's Digital Assets, Digital Information and Accounts for Company Business only except for limited usage defined in section 6 of this Policy.
- 1.3 Personnel and Excluded Contractors must not share their TC Energy Individual Accounts or allow unauthorized access to the Company's Digital Assets.
- 1.4 Personnel and Excluded Contractors must not create, transmit or store non-public Company Information on non-TC Energy Accounts.
- 1.5 Personnel and Excluded Contractors must not use the Company's Accounts to register for online services (e.g., social media, websites, shopping accounts) unless these services will be used for Company Business (e.g., accessing white papers, registering for government sites, Contractor's portals).
- 1.6 Personnel and Excluded Contractors must follow the Cybersecurity Password Standard for all Accounts on TC Energy-approved Digital Assets.

- 1.7 Personnel and Excluded Contractors must not attempt to change the security settings or otherwise alter security features of TC Energy's Digital Assets, Digital Information or Accounts without the prior written authorization from TC Energy's Cybersecurity Office (CSO). Personnel authorized to make such changes are identified in the Cybersecurity Policy.
- 1.8 Personnel must immediately follow actions regarding cybersecurity threats communicated by the CSO. Legitimate CSO communication is sent from TC Energy's Cyber Safety account (cyber_safety@tcenergy.com) or CSO's mailbox (cybersecurity_office@tcenergy.com).

2 TC Energy's Digital Assets

- 2.1 Personnel and Excluded Contractors must use only Company-approved Digital Assets, including non-TC Energy Digital Assets such as Software-as-a-Service, to access, create, view, modify, process, transport, transmit, receive, or store TC Energy's Digital Information. Excluded Contractors may only use non-Company Digital Assets in accordance with their legal agreement with TC Energy.
- 2.2 Personnel and Excluded Contractors must use only the Company-approved software on TC Energy's Digital Assets.
- 2.3 Personnel and Excluded Contractors must connect only approved Digital Assets that they are confident and have taken reasonable steps to ensure are free of malware, such as computer viruses, to other TC Energy Digital Assets and networks.
- 2.4 Personal and Excluded Contractors must take reasonable steps to appropriately secure and store TC Energy's Digital Assets at all times. This may include, but is not limited to, the proper use of a security cable or similar physical locking device, in a locked cabinet or in a room with limited and controlled access.
- 2.5 Personnel and Excluded Contractors must connect only TC Energy removable media (e.g., USB drives, CD/DVD/Blu-Ray players and discs, tablets, smartphones, etc.) to TC Energy Digital Assets.
- 2.6 Personnel and Excluded Contractors must ensure that any TC Energy removable media they use to transport or store Company Digital Information is encrypted.

3 Non-TC Energy Digital Assets

- 3.1 Personnel must not connect their personal or non-TC Energy Digital Assets to any TC Energy wired or wireless network (Corporate or ICS) except the Company's guest network. When Personnel connect their personal or non-TC Energy Digital Assets to the Company's guest network, the Company is not responsible for safety and security of such assets.
- 3.2 Excluded Contractors' Digital Assets may only be connected to TC Energy's Digital Assets if they are authorized by the Company as part of a legal agreement between TC

Energy and their employer containing Cybersecurity requirements for the use of those assets.

- 3.3 Personnel must connect only registered Bring Your Own Device (BYOD) Digital Assets to TC Energy's designated BYOD wireless networks.
- 3.4 Personnel must not connect (wired or wireless) their personal Digital Assets to any TC Energy Digital Assets.

4 Cybersecurity Incidents

- 4.1 All suspected or actual Cybersecurity Incidents involving TC Energy's Digital Assets or Digital Information must be reported immediately, either by calling the Service Desk at 1.888.546.3484 in Canada and the U.S. and 001.866.278.0555 in Mexico or using Joule to "Report Incident" or submitting a ticket through ServiceNow.

5 Cybersecurity Awareness

- 5.1 Personnel must complete the cybersecurity awareness training assigned by the CSO.
- 5.2 Personnel and Excluded Contractors must exercise due diligence detecting, avoiding, and reporting Social Engineering cyber-attacks, such as phishing, when using TC Energy's Digital Assets. Reporting of Social Engineering attempts can be done through Microsoft Outlook's Report-a-Phish icon or, when urgent, by calling the Service Desk at 1.888.546.3484 in Canada and the U.S. and 001.866.278.0555 in Mexico. Employees who do not exercise due diligence regarding Social Engineering cyber-attacks will be subject to the Phishing Corrective Discipline Process.
- 5.3 Contractors who do not exercise due diligence regarding Social Engineering cyber-attacks will be subject to the Phishing Corrective Discipline Process. This can result in revoking of their access to TC Energy's Digital Assets and facilities.

6 Personal Use of TC Energy Digital Assets and Digital Information

- 6.1 Personnel and Excluded Contractors must not use TC Energy's non-public Digital Information for personal purposes.
- 6.2 Personnel may use the Company's Digital Assets and Accounts for limited and reasonable personal use which:
 - a) is infrequent;
 - b) incurs no additional fees;
 - c) creates no direct or indirect interference with their responsibilities; and
 - d) has no negative impact on other Personnel and Excluded Contractors and/or TC Energy's operations, reputation, or Cybersecurity Posture.
- 6.3 The Company, its authorized Contractors and government agencies may monitor and inspect without notice all content Personnel and Excluded Contractors view, create, receive, or transmit using TC Energy's Digital Assets or Accounts.

- 6.4 TC Energy does not guarantee the maintenance, security, privacy, or recovery of personal Digital Information (e.g., contacts, photos, voicemail, documentation, email) on the Company's Digital Assets.

Your responsibility

Employees and Contractors must follow all applicable provisions and the spirit and intent of this corporate governance document and support others in doing so. Employees and Contractors must promptly report any suspected or actual violation of this corporate governance document through available [channels](#) so that TC Energy can investigate and address it appropriately. Employees and Contractors who violate this corporate governance document or knowingly permit others under their supervision to violate it, may be subject to appropriate corrective action, up to and including termination of employment or contract, as applicable, in accordance with the Company's corporate governance documents, employment practices, contracts, collective bargaining agreements and processes.

Interpretation and administration

The Company has sole discretion to interpret, administer and apply this corporate governance document and to change it at any time to address new or changed legal requirements or business circumstances.

Non-retaliation

TC Energy supports and encourages Employees and Contractors to report suspected violations of corporate governance documents, applicable laws, regulations, and authorizations, as well as hazards, potential hazards, incidents involving health and safety or the environment, and near hits. Such reports can be made through available [channels](#). TC Energy takes every report seriously and investigates it to identify facts and, when warranted, makes improvements to our corporate governance documents and practices. All Employees and Contractors making reports in good faith will be protected from retaliation, and all Employees and Contractors must report if they or someone they know is being or has been retaliated against for reporting. Good Faith Reporting will not protect Employees and Contractors who make intentionally false or malicious reports, or who seek to exempt their own negligence or willful misconduct by the act of making a report.

Definitions

Account means any identity, authentication mechanism or email address used for accessing any Digital Asset.

Individual Account means any Account that is intended to be used by a single person.

Company Business means all business activities undertaken by Employees and Contractors during the Company's operations or on the Company's behalf, on or off TC Energy's premises.

Contractor means a third party hired by TC Energy to perform services for or supply equipment, materials, or goods to the Company. Contractors include, without limitation, Contingent Workforce Contractors, and Excluded Contractors.

Contingent Workforce Contractor (CWC) means an individual who:

- is employed by a third party to work on behalf of TC Energy;
- uses TC Energy's assets (e.g., workstation, email, phone) and corporate services;
- is compensated on an hourly or daily rate basis (Canada and the U.S.) and monthly (Mexico); and
- works under the direction of a TC Energy leader.

Cybersecurity Posture means the cybersecurity status of TC Energy's Digital Assets and Information and the cybersecurity resources and capabilities in place to manage the Company's cybersecurity defenses and to respond to cybersecurity incidents.

Digital Asset means any network device, computer system, application, data storage systems, or service (and associated data required for operation). This includes, but is not limited to, laptops, tablets, smartphones, and removable media.

Digital Information means any Information that exists in a digital form.

Employee means full-time, part-time, temporary and student employees of TC Energy.

Excluded Contractor means a third party or individual employed by a third party who:

- delivers services, equipment, materials, or goods to the Company using their own tools and assets (e.g., workstation, laptop, email, phone, PPE, vehicle);
- does not increase TC Energy corporate headcount and overhead costs;
- does not use TC Energy's assets and corporate services; and
- directs their own work or receives direction from their employer.

Good Faith Reporting means an open, honest, fair, and reasonable report without malice or ulterior motive.

Cybersecurity Incident means an occurrence that can jeopardize the confidentiality, integrity, or availability of a Digital Asset or Digital Information or constitutes an imminent threat or violation of this Policy and associated Cybersecurity Standards.

Industrial Control Systems (ICS) Environment means integrated information technology and operational technology systems used in industrial production that achieve a prescribed value for a variable through deliberate guidance or manipulation. ICS Environment includes Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs) and other types of industrial measurement and control systems.

Information means any content, data, materials, or document created or received during Company Business, regardless of the source, medium or form (printed or electronic, including instant and text messages).

Inter-Affiliate Codes means, collectively, the TC Energy Canadian Gas Pipelines Code of Conduct, the TransCanada PipeLines Limited Canadian Mainline Bid Floor Personnel Information Policy, the U.S. Federal Energy Regulatory Commission Standards of Conduct for Transmission Providers, the U.S. *Interstate Commerce Act*; and the TC Energía Code of Conduct.

Personal Information means any information on its own or when combined with other information, which can be used to identify an individual. For the full definition, see the Protection of Personal Information Policy.

Personnel means Employees and Contingent Workforce Contractors of TC Energy.

Software-as-a-Service means capability to use the provider's applications running on a cloud infrastructure.

Social Engineering means the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

TC Energy or the **Company** means TC Energy Corporation and its wholly owned subsidiaries and/or operated entities.

References

Related corporate governance and supporting documents

- Code of Business Ethics Policy
- Cybersecurity Password Standard
- Cybersecurity Policy
- Cybersecurity Standards
- Data and Information Policy
- Phishing Corrective Discipline Process
- Protection of Personal Information Policy

How to contact us

- IS Service Now
- [Policy Questions and Comments](#)
- Service Desk

TC Energy's reporting channels

- [Ethics Helpline](#)
- [Corporate Compliance](#)
- [Internal Audit](#)
- Human Resources
- Legal department
- Compliance Coordinators