# Technology Requirements for Suppliers and Contractors

*Effective Implementation: August 17, 2021*

**TECHNOLOGY REQUIREMENTS:**
This document establishes a uniform requirement for use of the Equitrans' technology resources to ensure the integrity and security of such resources and related Company information.

**SCOPE:**
Equitrans' agents, vendors, contractors, consultants, suppliers and other entities or parties who have access to technology resources and/or Company information.

**REQUIREMENT DETAILS:**

## I. DEFINITIONS

A. For purposes of this document "**Technology Resources**" shall mean all hardware (i.e., laptop and desktop computers, printers, scanners, desk telephones, cell phones and mobile devices, servers, etc.), software, application systems, network systems, and other information technology, operational technology, and telecommunication systems, including technologies that are provided as a "service" via the Internet provided by Equitrans.

B. For purposes of this document "**Company Information**" shall mean all information used, created, or received in the conduct of Equitrans business which is electronically generated, stored, transmitted, or processed using Technology Resources.

C. For purposes of this document "**User**" shall include, but not be limited to, contractors, consultants, agents, vendors and any other individual or entity using Equitrans' technology resources.

## II. PRIVACY

A. Equitrans employs monitoring capabilities for the purposes of ensuring operational stability, security, and appropriate use. Use of technology resources, including the use of the Internet, may be monitored and reviewed on a regular basis to ensure compliance with all internal and external laws, rules, regulations, policies, standards, and guidelines.

B. By using technology resources (as defined above), users agree to allow Equitrans to monitor their activities and to disable or suspend those activities, including active network connections or access to systems and data, as required.

C. Equitrans reserves the right to access and disclose all messages sent via its electronic mail system for any purpose at any time. Equitrans may also disclose electronic mail messages to law enforcement officials without prior notice to users who may have sent or received such messages.

## III. ACCESS TO TECHNOLOGY RESOURCES

A. Access to technology resources is restricted to users with a legitimate business need. Access will be requested by the user's manager/supervisor and approved by the owner of the resource.

B. Any access to technology resources or Company information not relevant to the user's engagement must be reported immediately. User must exit out of all technology resources and contact Equitrans IT.

C. Equitrans requires authentication to utilize all technology resources, whether owned and managed by Equitrans or provided as a service to Equitrans. This includes access to networks, servers, file systems, applications systems (on-premise or cloud-based), and enterprise email and file management applications such as Office 365.

D. Passwords must be constructed according to the following required length and complexity requirements:

   i. passwords must contain a minimum of 12 characters in length and must include three of the following four elements: *upper- or lower-case letters*, *numbers*, and *special characters*

   ii. the maximum lifespan permitted for a password is 90 days, regardless of the information technology being accessed

   iii. a previously used password may be re-used after 12 password cycles

E. Users should refrain from using the same password across multiple information technologies.

F. Multi-factor authentication is also required as an additional security measure where configured

G. Each User is responsible to:

   i. maintain the confidentiality of his/her user ID and password;

   ii. ensure that his/her user ID and password are not used by other individuals to access technology resources;

   iii. adhere to the established user ID and password protocols; and

   iv. lock or disable access to technology resources when unattended.

H. Passwords should not be written down or stored electronically in an unencrypted manner. Passwords should never be kept in spreadsheets or stored locally on a computer or in file systems.

I. The use of password vaults other than Company-provided solutions is prohibited. Access to the Company-provided password vaulting solution can be requested by the user's manager/supervisor.

J. Users are sometimes prompted by browsers (Internet Explorer, Chrome, etc.) to save passwords to websites. This practice is not considered secure and is prohibited.

K. Users are responsible for ensuring that passwords are not exposed while being entered into login screens.

L. Passwords must not be transmitted across networks or systems via email and/or in an unencrypted manner.

## IV. TECHNOLOGY RESOURCES ACQUISITION AND USE

A. Equitrans-supplied technology resources are owned by Equitrans and are provided for use where appropriate. Equitrans is committed to minimizing the acquisition, maintenance, and support costs of its technology resources and ensuring that technology resources are deployed in an efficient, cost-effective, operationally sound, and secure manner.

B. Unless specifically approved otherwise, all technology resources are to be sourced from, configured by, and installed by the IT Department.

C. Technology resources that have not been authorized for purchase or use, does not meet minimum technical standards to operate efficiently/effectively, or pose a risk to Equitrans will be deactivated and/or removed.

D. Users are prohibited from making alterations to installed technology resources, including the removal of hardware or software components.

E. Technology resources may be regularly scanned for inventory purposes, to make necessary upgrades or reconfigurations, or to identify unauthorized hardware or software configuration changes.

F. Users must not circumvent technology resources' security controls, measures, or programs implemented to prevent, detect, or remediate security threats.

G. Under no circumstances should users install, configure, or use hacking software or software intended to do harm to Equitrans or to another organization.

H. Mobile devices and related software applications are subject to the same standards and guidelines as above.

   i. All Company mobile devices must be enrolled in mobile data management before deployment.

   ii. Users should only source mobile device software applications from Equitrans' Company portal. All other applications must be approved in advance for Company use.

I. Hardware Tracking and Maintenance

   i. All Company end-user hardware (laptops, desktops, and mobile devices) must be configured by and assigned to users by the Service Desk.

ii. Upon termination of agreement or contract,), all technology resources must be returned to the Equitrans Service Desk, including laptops, desktops, mobile phones, and mobile devices (iPads, tablets, and mobile hotspots).

iii. To ensure information technologies are replaced, maintained, and upgraded regularly, IT utilizes an asset management process.

1. Hardware and related software may be regularly scanned for inventory purposes, to make upgrades as necessary, or to identify any unauthorized configuration or software changes.
2. Equitrans reserves the right to remove any unauthorized hardware or software changes as necessary, or to reconfigure hardware or software to meet current Company standards.

iv. All repair and maintenance of Company end-user hardware (laptops, desktops, and mobile devices) is prohibited unless authorized and coordinated by the Service Desk.

J. Physical Security of Hardware

i. Users are responsible for the physical security of Company-issued hardware (laptops and mobile devices) when in non-Company locations.

ii. Users are responsible to report lost or stolen hardware to the Service Desk immediately.

## V. APPROPRIATE USE OF INTERNET RESOURCES

Equitrans provides access to the Internet primarily for business purposes. Incidental and occasional use of the Internet is permitted, provided that such use does not violate supplier code of conduct guidelines, negatively affect employee productivity, or result in observable service degradation.

A. Equitrans maintains a list of Internet sites that are considered offensive or inappropriate for use and reserves the right to block access to these sites as necessary.

B. Equitrans maintains a list of countries from which Internet and email traffic may put the organization at risk and reserves the right to block Internet, login, and email traffic to/from those countries.

C. Users may not bypass, disable, or tamper with Equitrans' restrictions on Internet sites or countries, or block the ability to monitor Internet use in any way.

D. Users may not install or use software intended for the purpose of attacking or harming the technology infrastructure of another organization via the Internet.

E. Users may not install or use software intended to conceal or anonymize a user's identity while using the Internet.

## VI. APPROPRIATE HANDLING OF COMPANY INFORMATION

Company information is intended for use in conducting Equitrans' official business. Users accessing Company information agree to comply with any applicable supplier code of conduct

guidelines, laws, and regulatory obligations and to satisfy Equitrans Information's confidentiality, integrity, and availability requirements.

Equitrans Midstream is the owner of all Company data and entrusts users to use and safeguard such data as appropriate:

A. Company information, including Personally identifiable information (PII), may only be stored, transmitted, or processed via Company-approved and supported methods, services, and storage locations. Contact the IT department to determine appropriate storage locations and methods.

B. IT must be notified of all data received and stored on Equitrans technology containing Personally identifiable information (PII).

C. Users may not use their own personal data hosting services for storage of Company information.

D. The use of data and file hosting services (other than those provided by Equitrans) are prohibited unless specifically approved for a Company-defined business need and approved by IT. Examples of common cloud data storage providers that are prohibited unless approved by IT include Google Drive, Dropbox, and iCloud, as well as notetaking storage providers such as Evernote.

E. Data may not be transferred to an external business partner or third party via the use of the partner or third-party's data hosting service unless approved by IT in advance.

F. All methods to store, transmit, or process Company information must provide for encryption while in transit or at rest.

G. The transfer of data to third parties must be performed via Company-approved methods, including the use of secure file transfer protocols or data hosting services.

H. The use of physical media (such as USB drives) to store or transmit Company information is prohibited unless pre-approved.

I. Data in Transit (to Third Parties)

    i. Business needs often require Equitrans to package data and transmit it to a third party. When approved by IT, Company data must be transmitted to and from the third party in a secure, encrypted fashion, and while in the third party's custodianship, is subject to all the provisions for data-at-rest.

J. Secure File Transfer Protocol (SFTP) and Site-to-Site VPN (StSVPN)

    i. Equitrans employs SFTP tools for encrypted and secure transmission of data from point-to-point or system-to-system. Use of this tool can be requested from the Service Desk. Equitrans data to be transmitted is subject to the restrictions noted elsewhere in this document.

K. Use of physical media

i. The use of physical media is prohibited unless approved by IT as it is considered the least secure method of transmitting Company data. However, in some cases, it is appropriate to move data using this method. Contact your supervisor or the IT department to determine an appropriate method to transfer data.

L. Data Transfers to Equitrans (from Third Parties)

i. In many cases, Equitrans needs to receive data from third parties. Data received from third parties may not have been subject to the same level of controls as Equitrans requires, therefore caution in introducing such data to Equitrans' technical infrastructure is required. When data is being transferred into Equitrans' environment, the following considerations should be given:

1. Use the most appropriate method for the data transfer. Data being received by Equitrans should be transmitted in as secure a manner as possible so that the data cannot be corrupted or modified in transit.

2. Scan data for vulnerabilities and malware before introducing it to Equitrans' technical infrastructure. All data that is received by Equitrans and is to be introduced to file shares, application systems, data storage, etc. must be scanned for vulnerabilities and malware in advance.

3. If the data is contained on a USB, it must not be transferred to a laptop or desktop without first contacting IT.

4. Validate data before use. All data received by Equitrans should be verified for accuracy, integrity, and completeness before accepted into Equitrans' technical infrastructure.

M. Data Destruction

i. All data that is transmitted from Equitrans or received by Equitrans is subject to record retention guidelines. Contact your supervisor or the IT department to determine appropriate record retention guidelines.

## VII. CYBERSECURITY

Equitrans employs information technologies, methods, and safeguards intended to prevent or detect the intentional disclosure, modification, or destruction of data, or disruption of critical business processes, technologies, or facilities. Users are responsible to use technology resources in a secure manner and adhere to policies for safeguarding Equitrans' technology and information assets.

A. Cybersecurity technologies, such as anti-malware software, network access control software, and all other desktop programs must remain installed, enabled, and regularly updated on all technology resources. Users may not bypass, disable, or tamper with these technologies.

B. Users must exercise caution when opening email messages and attachments from unknown sources. These data files or attachments may contain viruses or other malicious

software which pose a risk to Equitrans. Any phishing or suspicious emails must be reported to Equitrans Cybersecurity via the embedded email reporting capabilities.

## VIII. MISUSE/MISAPPROPRIATION OF TECHNOLOGY RESOURCES

Misuse or misappropriation of Equitrans' technology resources is strictly prohibited. Examples include, but are not limited to:

A. Use of technology resources that violates supplier code of conduct guidelines, rules, or administrative orders, or is used for illegal or unlawful purposes.

B. Use of technology resources to misrepresent Equitrans or to interfere with the proper business use of technology resources by other users.

C. Use of technology resources for which the user does not possess appropriate or sufficient rights or permissions.

D. Use of technology resources to: (1) further the personal business interests of the user or any other business use that is not directly related to the business of Equitrans; (2) violate existing copyright laws or engage in other unlawful activity; and/or (3) conduct unauthorized downloading or copying of Company information.

E. Use of technology resources to: (1) represent the user's personal opinions and thoughts as those of Equitrans; (2) transmit chain letters or bulk or large-scale unsolicited e-mails; and/or (3) transmit material or information that is or may be considered profane, obscene, abusive or otherwise offensive.

F. Use of e-mail systems to: (1) download or distribute content that is considered offensive, insulting, harassing, discriminatory, or in violation of supplier code of conduct guidelines; (2) transmit chain letters or bulk or large-scale unsolicited e-mails; (3) view, copy, alter, or delete e-mail account belonging to another User and/or (4) to further personal business interests.

G. Intentional or malicious destruction, modification, or manipulation of technology resources.

H. Excessive use of technology resources that interferes with job performance or negatively impacts business operations, including use for personal business or gain.

## IX. TECHNICAL REQUIREMENT VIOLATIONS

Violations of these technical requirements may result in loss of privileges to technology resources and disciplinary action, including without limitation, termination of contract.