Information Technology (IT)
Security Policy Definitions

IT Resource: Any staff, technology, data, software, physical or virtual locations, financial assets or any other element that delivers IT services.

IT Asset: A physical/virtual device or location used by staff to perform work, including servers and server rooms, physical networks, desktops and laptops, communications closets and gear, and Personal Digital Assistants (PDAs).

Critical IT Asset: An asset required to support critical Community Transit operations in the immediate (72 hours or less) future.

Least Privilege: Principle that states a user is given access to and authorization only for the data or asset(s) required to perform the user's job duties.

Data Owner: The operational manager who holds responsibility for a specified set of data and who is held responsible for loss or damage to that data. The data owner defines access, retention, availability, integrity, and confidentiality rules for the data.

Data Custodian: The person who maintains the data, including backups, enforcement of access rules, and any other activities supporting the availability, integrity, and confidentiality constraints specified by the data owner.

Sensitive Data: Any data that requires special access protection, such as data about individuals, infrastructure, financial, or security. It also includes data for which licensing restrictions exist and disclosure is not allowed (e.g. software keys, licensed GIS data, etc.).

Critical Data: Any data which requires special backup/restore considerations for disaster recovery, generally that data required to minimally operate Community Transit in an emergency.

Electronic Communication: Any means by which data moves between Community Transit and any outside Information Technology (IT) assets, or between Community Transit assets, including network, telephone, thumb drive, laptop, DVD, printer, or fax.

This policy applies to anyone accessing or using Community Transit IT resources.

1. IT Department May Monitor Use of Resources

Use of IT resources owned by Community Transit may be monitored, copied, or recorded without warning with approval of Community Transit IT or Human Resource (HR) management. Users do not have an expectation of privacy when using Community Transit owned resources. Any software or hardware which primarily or incidentally can be used to obscure or remove any historical, tracking, or location information (e.g., portable applications) is prohibited unless specifically permitted by Information Technology.

Use of personal devices on the Community Transit network is restricted to only the portions of the network where such devices are explicitly allowed. Use of the network or access to Agency data by these devices may be monitored. Community Transit reserves the right to inspect personal devices which are or have been attached to the Community Transit network.

2. Unauthorized Use of Personal or Account Information is Prohibited

Users may not disclose their personal authentication (such as passwords or PINs) or account information for data to others without IT management approval. Generic user IDs shared between multiple users may only be used with the CTO's permission.

3. Users Will Follow All Rules for Vendor-Owned Data

Users must follow all access and use restrictions of vendor-owned data set forth in the vendor contract.

4. Only Agency-Approved Devices May be Attached to IT Resources

No equipment (such as non-IT servers, desktops, mobile devices, or printers) may be attached to Community Transit network resources without express authorization from IT. Use of external storage devices (such as USB flash drives) is generally discouraged because of security risks; please contact IT for current guidelines.

Deliberate or reckless introduction of incorrect or damaging data or software (such as spyware, chain e-mails, private network access such as LogMeIn, or IM viruses) is prohibited. Deliberate or reckless activities that could damage Community Transit IT resources are prohibited. These activities include:

- Careless treatment of an IT resource.
- Loss due to failure to secure an IT resource.
- Unauthorized changes to an IT resource.
- Any other actions that may make the resource become unusable.
- Any attempt to bypass Agency security functions or processes.

5. Access to Community Transit Data is Based on Least Privilege

The principle of least privilege implies access and authorization permissions are tied to a job, not to an employee. Employees and contractors will have access only to data which is:

- Generally available to employees and contractors.
- Required by an employee or contractor to perform assigned job duties.

Community Transit data is classified by the data owner as sensitive/non-sensitive and critical/non-critical:

- If any element in a data store is sensitive and/or critical, the data store is considered sensitive and/or critical.
- Employees and contractors with access to sensitive or critical data receive necessary training in special handling of the data prior to access being given.
- If external parties require access to Community Transit data, a protocol for that access is developed by the data custodian, with approval by the data owner, to cover allowed access, required non-disclosure agreements, who can use the data, and any other necessary parameters. This protocol must release only the minimum required data.
- All external access protocols must conform to Community Transit policy. If the access is limited to a specific project, the standard is reviewed as part of the project closeout and either expires or is re-issued as a permanent interface standard. If the access is ongoing, it must be periodically re-evaluated for compliance by the data custodian, in coordination with the data owner.

6. Electronic Access Based on Least Privilege Principle

Access to Community Transit's electronic communication resources is established by the principle of least privilege.

7. Identifiable Logins Are Required to Create, Modify, or Delete Data

No production data may be created, modified, or deleted under a generic ID.

8. Community Transit Houses Sensitive Information in Data Stores

No data store containing sensitive data may be external to the Community Transit corporate firewall unless that data store can be verified as secure according to Community Transit requirements.

No data store containing sensitive data may be stored on removable media or hardware that may be removed from Community Transit secured space unless the data has been encrypted or redacted by scrambling or overwriting the sensitive data.

9. Sensitive Data Cannot Be Released Without Authorization

Sensitive data cannot be released unless authorized.

No user provided access to sensitive data may provide that data to any non-authorized user. This includes leaving sensitive information visible on-screen or on printed media which a non-authorized user could access.

Any loss of sensitive data must be reported immediately.

10. Critical Data Losses Must Be Reported Immediately

Any loss of critical data must be reported immediately.

11. Access by External Parties Must Comply with Community Transit Policy

If external parties require access to Community Transit resources through electronic communication resources, a protocol for that access is developed by Community Transit to cover allowed access, who can use the access, and any other necessary parameters. All access must conform to Community Transit policies.

- If the access is limited to a specific project, the protocol is reviewed by Community Transit as part of the project closeout and either expires or is re-issued as a permanent interface protocol.

- If the access is ongoing, it must be periodically re-evaluated by Community Transit for compliance.

12. Community Transit Minimizes Sensitive Data Exposure Risk

Transmission of sensitive data through any unsecured network or electronic communication facility not under Community Transit control must be encrypted.

13. Community Transit Does Not Send Sensitive Data to Unsecure Locations

Sensitive data must not be transmitted to an insecure destination (such as printing sensitive data in a publicly accessible area).

14. Access to Assets is Based on Least Privilege

Access to any Community Transit asset is based on least privilege. Employees and contractors will have access only to assets which are:

- Generally available to employees and contractors.
- Required by that employee or contractor to perform assigned job duties.

15. Only Authorized Users May Access Assets

IT assets may be used by anyone authorized for that asset (for example, someone else may use your workstation if theirs is unavailable and you're on vacation). In all cases, users are required to use their own authentication credentials regardless of the Community Transit IT asset they use.

Contractors or third-parties accessing secured physical Community Transit IT assets must be signed in and managed by a Community Transit employee.

If external parties require access to Community Transit IT assets, a protocol for that access is developed by the data custodian (with data owner approval) to cover allowed access, wh**o can use the access, and any other necessary parameters. All access must conform to Community Transit policy.**

- If the access is limited to a specific project, the protocol is reviewed as part of the project closeout and either expires or is re-issued as a permanent interface protocol.
- If the access is ongoing, it must be periodically re-evaluated for compliance.

16. Sensitive Data May Not Leave Community Transit

Any Community Transit IT asset holding critical or sensitive data may not leave Community Transit control until that critical or sensitive data is securely removed.