



## ***Ensuring Digital Security***

### **POL-TC-4001**

Section 1:	User's Responsibilities to Protect Technology Assets.....	3
1.1.	Adhere to Policy.....	3
1.2.	Community Transit's Technology Assets Must Remain Within Control of the Agency.....	3
1.3.	Report Misuse, Unauthorized Access, Theft or Loss of Technology Assets.....	3
1.4.	Software or Hardware Acquisition Must be Approved.....	4
1.5.	Protect Credentials.....	4
1.6.	Use Strong Passwords.....	4
1.7.	Lock Computer Screens When Leaving Computer Unattended.....	4
1.8.	Complete Annual Security Awareness Training.....	5
Section 2:	Managing Access to Technology Assets.....	5
2.1.	Data Centers, Network and Telecommunications Rooms, and Information Technology Storage Locations are Restricted.....	5
2.2.	The Information Technology Department Tracks Technology Assets.....	5
2.3.	System Access May Require Multiple Factors for Authentication.....	5
2.4.	System Access for Some User Accounts Is Limited.....	5
2.5.	The Information Technology Department May Monitor Use of Technology Assets.....	6
2.6.	Personal Use of IT Resources is Allowed Within Limits.....	6
2.7.	Use of Personal or Non-Agency Devices on the Agency Network is Restricted.....	6
2.8.	Accessing Agency Technology Assets from Personal Devices Requires Current and Patched Operating System.....	7
2.9.	Lockout Methods will be Used to Safeguard Agency Assets.....	7
Section 3:	Administering this Policy.....	7
3.1.	The CEO Approves Policy Content Revisions.....	7
3.2.	The Chief Technology Officer Approves Supplemental Information Relevant to This Policy.....	7
3.3.	The Chief Technology Officer Approves All Exceptions to This Policy.....	7
3.4.	Department Directors and Their Delegates Communicate and Ensure Compliance to This Policy.....	8
3.5.	The Chief Information Security Officer Develops and Implements a Digital Security Program.....	8
3.6.	The Information Technology Department Approves and Implements Technologies.....	8
Section 4:	Appendix.....	8



## ***Ensuring Digital Security***

**POL-TC-4001**

### **Definitions:**

**Credentials:** The individual factors collectively used to identify a user, system, or application, including but not limited to username, password, pin, biometric data, keycard, or assigned physical key.

**Critical Data:** Data elements vital to the successful operation of the organization. Typically, critical data requires special backup/restore considerations for disaster recovery. An organization may define its Critical Data elements as those that represent protected personal information, those that are used in financial reports or regulatory reports, the elements that are critical for a decision-making process, or the elements that are used for measuring organizational performance.

**De Minimis:** Use or cost to the agency that is so small as to be insignificant or negligible.

**Jailbroken Device:** An Apple device with restrictions removed to access low-level functions.

**Least Privilege:** A 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.

**Passphrase:** A passphrase is like a password, but longer and more secure. It is typically more than 15 characters and is a phrase or sentence that is made up of multiple words that is easier to remember than complex passwords.

**Phishing:** A form of social engineering that uses email or malicious websites to solicit personal information or to persuade downloads of malicious software by posing as a trustworthy entity.

**Routed Device:** An Android device with restrictions removed to access low-level functions.

**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.).

**Technology Asset:** Assets that fall under the purview of the Information Technology Department. A combination of digital assets such as Agency owned data, software, databases, virtual machines, and other non-physical assets, as well as physical assets (such as computer hardware, phones, mobile devices, printers and any other information technology equipment, servers, networks, and storage devices including USB sticks and other portable storage devices).

**User:** Anyone legitimately accessing or using agency technology assets including employees, temporary personnel, contractors, and vendors.

This policy applies to anyone accessing or using Community Transit technology assets.

**Section 1: *User's Responsibilities to Protect Technology Assets.*****1.1. Adhere to Policy.**

Digital security is everyone's responsibility whether it be at work or remotely connected. It is essential for the agency and user's own personal digital safety. While the Information Technology Department can do a lot to protect employees, they depend on the awareness of all users to help safeguard agency technology assets from risks associated with loss of control of these assets. These policies are intended to:

- Conform to the business goals of Community Transit as defined by the Board of Directors and agency Executive Leadership Team
- Assure reliable and timely availability of technology assets
- Store and transmit data accurately and securely
- Establish best practices for using technology assets

**1.2. Community Transit's Technology Assets Must Remain Within Control of the Agency.**

Except for technology intended for mobile use (such as laptops and mobile phones), users may not move physical technology assets without obtaining permission from the Information Technology department through the Service Desk.

Removable media (e.g., USB sticks) purchased for use on agency computers must not be used on non-agency computers. Removable media from external sources should be evaluated by the Information Technology department prior to use.

Users may not automatically forward email to a third-party email system. Individual messages forwarded must not contain confidential agency information.

Release of technology assets and data to external parties must be authorized by the appropriate custodian of the asset or data.

All sensitive or critical information sent over the public Internet must be encrypted during transport. Technology assets holding critical or sensitive data may not leave agency control until that data has been securely wiped from the asset.

The Information Technology Service Desk must be informed of all instances where sensitive data is to be transmitted to external parties (routine or one-time), which will be reviewed, approved, and tracked by the Chief Information Security Officer. The intent is to understand the method by which sensitive information is being sent. Once approved, similar sensitive information can be sent via the same method without informing the Service Desk.

**1.3. Report Misuse, Theft or Loss of Technology Assets.**

All users are required to report the misuse of technology assets including physical careless treatment or inappropriate use of the device. Deliberate or reckless introduction of incorrect or damaging data or software is prohibited. Technology assets that are lost or stolen must be reported immediately to the Information Technology Service Desk.

**1.4. Report Unauthorized Access of Technology Assets.**

Users who know of or suspect unauthorized access to technology assets must report it immediately. Any user suspecting that his/her password may have been compromised must immediately report the incident and change all similar passwords.

**1.5. Software or Hardware Acquisition Must be Approved.**

Users may not purchase hardware or install/use software on agency owned physical technology assets without prior approval from Information Technology. The acquisition of any hardware or software (including software as a service) requires an evaluation by the Information Technology Department prior to acquisition, regardless of cost (including free services). Contact the Service Desk to request a review.

**1.6. Protect Credentials.**

Users may not disclose their credentials (usernames, passwords, keycards, etc.) to anyone including other employees, supervisors, Information Technology Service Desk staff, and anyone outside of Community Transit. Users cannot write down or otherwise expose credentials in an insecure (non-encrypted) manner.

The Information Technology Department offers an approved method for users to store their credentials. Contact the Service Desk for more information.


**1.7. Use Strong Passwords.**

Passwords make up part of the keys used to access technology assets. While the Information Technology department puts some conditions on aspects of passwords (such as requirements on the minimum length and complexity), users are encouraged to go further to ensure their passwords protect the technology assets they access:

- Do not use dictionary words, proper names, number or character patterns, or common number sequences.
- Do not use your username or any portion of your name.
- Do not use easily guessed personal information such as names of family members, pets, birth dates, etc.
- Whenever possible use a lengthy passphrase that you can remember. Due to the length, 'cracking' techniques that hackers can use to derive shorter, even complex, passwords are ineffective with passphrases. For better security, no part of it should be derivable from personal information about the user or his/her family or be 'common' phrases found in literature or popular culture.

Passwords for externally hosted business systems must minimally comply with current Information Technology Department standards for password length, complexity, and expiration even if the external system standards are less.

**1.8. Lock Computer Screens When Leaving Computer Unattended.**

While the Information Technology Department configures computers to lock after a certain period of inactivity, users are required to lock their computer screens when leaving their computer unattended for any period. This can be accomplished by simultaneously pressing the Windows  and the "L" keys on your keyboard.

**1.9. Complete Annual Security Awareness Training.**

All employees are required to complete security awareness training upon hire, and those with regular access to computers must complete annual re-training. Content in this training provides a reminder of the security threats faced every day, and it is regularly updated to cover new avenues of attack.

**Section 2: *Managing Access to Technology Assets*****2.1. Data Centers, Network and Telecommunications Rooms, and Information Technology Storage Locations are Restricted.**

Individuals who do not have regular access to these locations must be escorted. Access must be documented by sending an email to the Chief Information Security Officer through the Information Technology Service Desk noting the individual's full name, agency, purpose, time of access, and escort. Refer to POL-SE-0010 "Accessing Community Transit Facilities by Authorized Contractors" for more information.

**2.2. The Information Technology Department Tracks Technology Assets.**

The Information Technology department maintains an inventory of all technology assets and tracks them in a Configuration Management Database.

**2.3. System Access May Require Multiple Factors for Authentication.**

Users may be required to provide multiple factors to authenticate on certain technology assets. This could include not only username/password, but also biometrics such as fingerprint reader or facial recognition, key card with a magnetic stripe or digital chip, token sent to an email account or as a text, token read from or pushed from a third-party authenticator application, and others. Users should protect access to these other factors similarly to protections for passwords.

**2.4. System Access for Some User Accounts Is Limited.**

Access to agency technology assets is based on least privilege. The principle of least privilege implies access and authorization permissions are tied to a role, not to a user. In addition:

- Technology assets may be used by anyone authorized for that asset. As an example, someone may access a workstation normally assigned to another employee if their workstation is unavailable and that employee is on vacation.
- The Service Desk does not create group accounts where multiple people login with the same credentials. Service accounts required to support systems are exempted.
- Anyone using a guest account must not have access to sensitive information.
- Information Technology department staff must use alternative accounts for administration of information systems. These alternative accounts must have a different password from the regular user account for the same user.

- Users who separate or have separated from service with Community Transit must have their access rights disabled or removed on or before the date of separation. Supervisors should contact the Service Desk with the request.
- Information Technology department staff may suspend access for any user at the request of Employee Engagement management or a member of the Executive Leadership Team.

**2.5. The Information Technology Department May Monitor Use of Technology Assets.**

Use of agency technology assets may be monitored, copied, or recorded without warning with approval of Information Technology, Employee Engagement or Risk Management. By using agency technology assets, employees understand and agree that there is no expectation of any privacy or confidentiality in any information created, stored, or transmitted using these resources, including any electronic communications which would be considered privileged, such as between the employee and the employee's attorney or health care provider.

Any software or hardware which primarily or incidentally can be used to obscure or remove any historical, tracking, or location information is prohibited unless specifically permitted by the Information Technology department.

**2.6. Personal Use of IT Resources is Allowed Within Limits**

Employees may use agency Information Technology resources for de minimis personal use if that use:

- Does not violate any agency policy.
- Does not limit or prevent anyone from performing their duties.
- Does not incur extra costs for the agency.
- Is separate from agency production data.
- Is not for individual profit or political advocacy.
- Does not expose the agency to legal liability (e.g., accessing pornography; trade secrets; unlicensed software; obscene, harassing, defamatory, or racist materials; engaging in online gambling).
- Does not represent employee as speaking on behalf of the agency.

Community Transit is not responsible for the integrity, availability, or confidentiality of personal data.

**2.7. Use of Personal or Non-Agency Devices on the Agency Network is Restricted**

Use of personal or non-agency owned devices on the agency network is restricted to only the portions of the network where such devices are explicitly allowed (i.e., public Wi-Fi). Use of the network or access to agency technology assets by these devices may be monitored. Community Transit reserves the right to inspect personal devices which are or have been attached to the agency network. Physically plugging in personal or non-agency owned devices to network wall jacks at any agency facility without prior

Information Technology authorization is strictly prohibited. Plugging devices into power outlets for charging purposes is permitted.

**2.8. Accessing Agency Technology Assets from Personal Devices Requires Current and Patched Operating System.**

Users who wish to access agency technology assets from personal devices must make sure those devices have a current supported operating system and that the operating system is patched with the latest security patches. Devices cannot be jailbroken, rooted, or otherwise compromised. This includes mobile devices and computers used to remotely connect to the network.

**2.9. Lockout Methods are Used to Safeguard Agency Assets.**

Information Technology implements methods that lock devices, accounts, or network ports after a certain number of failed attempts to prevent possible unauthorized access to agency resources. Some of these methods may require the user to contact the Information Technology Service Desk to regain access.

**Section 3: Administering this Policy**

**3.1. The Chief Executive Officer (CEO) Approves Policy Content Revisions.**

While the CEO approves policy content revisions, the Chief Technology Officer approves housekeeping adjustments, such as changes to employee titles or content changes required to comply with Board resolutions, regulations, or other valid requirements. Executive department staff posts the revised policy to the agency's official policy repository.

**3.2. The Chief Technology Officer Approves Supplemental Information Relevant to This Policy.**

The Chief Technology Officer creates and manages the agency's information technology framework. As part of that framework, the Chief Technology Officer oversees the development and maintenance of digital security policies. In addition, the Chief Technology Officer oversees the development of and approves technical procedures, standards, guidelines, and baselines that are captured in this policy's appendix. Changes to these may occur and be approved without an associated change to the primary content of the policy.

**3.3. The Chief Technology Officer Approves All Policy Exceptions.**

Request for exceptions to any part of this policy are submitted by completing the Policy Exception Request Form and emailing it through the Information Technology Service Desk to the Chief Information Security Officer for review and approval. The Chief Information Security Officer reviews, requests revision if needed, completes a risk analysis, and then submits to the Chief Technology Officer for determination.

**3.4. Department Directors and Their Delegates Communicate and Ensure Policy Compliance.**

While the Chief Technology Officer can direct the implementation of some protective measures that would apply to anyone accessing or using agency technology assets, it is only the leadership, management, and staff within each department that has the knowledge and understanding of how technology assets are being used. Ensuring Digital Security is everyone's responsibility.

**3.5. The Chief Information Security Officer Develops and Implements a Digital Security Program.**

As part of the Digital Security Program, the Chief Information Security Officer makes recommendations for revision of policies, procedures, tasks, and forms relevant to this policy with the intent of adapting the agency's security posture designed to protect enterprise communications, systems, and assets from both internal and external threats.

**3.6. The Information Technology Department Approves and Implements Technologies.**

Many of the tools and systems implemented by the Information Technology Department either directly or indirectly assists with adhering to portions of this policy for anyone accessing or using agency technology assets.

**Section 4: Appendix**

The appendix is stored as a separate password protected file and is not for distribution outside of Community Transit. It provides details around specific technical procedures, standards, guidelines, and baselines the Information Technology Department has put in place. Contact the Service Desk for access to the appendix.

Approved by: <u>Ric Ilgenfritz</u> Ric Ilgenfritz, CEO	Original Policy Written by: Mike Berman Technology Infrastructure Services Manager, IT
Cancels or Supersedes: Information Technology Security Policy, POL-TC-4001	
Last Reviewed by: Chief Technology Officer Policy Committee – February 9, 2022	
See Also:	



**Certificate Of Completion**

Envelope Id: FA5E2734C3C44A0F9D88D1D712E7E156

Status: Completed

Subject: Please DocuSign: POL-TC-4001 Ensuring Digital Security Policy.docx

Source Envelope:

Document Pages: 8

Signatures: 1

Envelope Originator:

Certificate Pages: 4

Initials: 0

Rachel Woods

AutoNav: Enabled

7100 Hardeson Road

Envelope Stamping: Enabled

Everett, WA 98203

Time Zone: (UTC-08:00) Pacific Time (US &amp; Canada)

rachel.woods@commtrans.org

IP Address: 206.208.64.20

**Record Tracking**

Status: Original

Holder: Rachel Woods

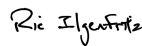
Location: DocuSign

2/15/2022 9:50:23 AM

rachel.woods@commtrans.org

**Signer Events****Signature****Timestamp**

Ric Ilgenfritz



Sent: 2/15/2022 9:56:17 AM

ric.ilgenfritz@commtrans.org

Viewed: 2/15/2022 10:00:05 AM

Chief Executive Officer

Signed: 2/15/2022 10:00:34 AM

Security Level: Email, Account Authentication  
(None)

Signature Adoption: Pre-selected Style

Using IP Address: 206.208.64.20

**Electronic Record and Signature Disclosure:**

Accepted: 2/15/2022 10:00:05 AM

ID: 9805d1dd-d1ba-4531-9bca-75da27cf2776

**In Person Signer Events****Signature****Timestamp****Editor Delivery Events****Status****Timestamp****Agent Delivery Events****Status****Timestamp****Intermediary Delivery Events****Status****Timestamp****Certified Delivery Events****Status****Timestamp****Carbon Copy Events****Status****Timestamp****Witness Events****Signature****Timestamp****Notary Events****Signature****Timestamp****Envelope Summary Events****Status****Timestamps**

Envelope Sent

Hashed/Encrypted

2/15/2022 9:56:17 AM

Certified Delivered

Security Checked

2/15/2022 10:00:05 AM

Signing Complete

Security Checked

2/15/2022 10:00:34 AM

Completed

Security Checked

2/15/2022 10:00:34 AM

**Payment Events****Status****Timestamps****Electronic Record and Signature Disclosure**

## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, Community Transit (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

### **How to contact Community Transit:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [Shawna.rose@commtrans.org](mailto:Shawna.rose@commtrans.org)

### **To advise Community Transit of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [kirsten.rising@commtrans.org](mailto:kirsten.rising@commtrans.org) and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

### **To request paper copies from Community Transit**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [Shawna.rose@commtrans.org](mailto:Shawna.rose@commtrans.org) and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

### **To withdraw your consent with Community Transit**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to [Shawna.rose@commtrans.org](mailto:Shawna.rose@commtrans.org) and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

### **Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

### **Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Community Transit as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Community Transit during the course of your relationship with Community Transit.