Accessing Community Transit Facilities by Authorized Contractors

POL-SE-0010 SECURITY & EMERGENCY MANAGEMENT

Definitions:

Access Badge: A physical proximity/smart card that identifies an individual and also allows them to use the access control system.

Access Control System: A system of hardware and software that includes badges, card readers, biometric devices, control panels, electronic door strikes, request to exit sensors, and other equipment that controls the access of individuals through doors, gates, vehicle bays, and elevators.

Access Level: A pre-defined level of privileges based on a legitimate business need and security assessment that allows individuals to unlock certain doors/gates/entrances and use devices assigned to the access control system.

Authorized Contractors: Contractors with an access badge, giving them access to non-public areas for an on-going period of time.

Community Transit Property: All property, buildings and bases that are owned, operated, or rented by Community Transit. This includes Operating Bases, Park & Rides & Transit Centers.

Excluded: A civil process where the Manager of Security & Emergency Management, their designee, or Transit Police identify and prohibit someone from being on Community Transit property.

Exterior Doors: The door through which an individual enters or leaves a building.

General Public: Any guest who comes to Community Transit and does not need access to non-public areas.

Key: A physical key used to gain access through a lock that is part of a mechanical key system.

Mechanical Key System: Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area.

Non-Public Areas: Areas located at community transit property that are not open to the general public.

Individuals: Community Transit authorized contractors.

Public Areas: The areas located at Community Transit property that are open to the general public during normal business hours. After hours, these locations are considered closed to the general public.

Restricted Area: Areas of Community Transit property that are restricted to only certain Individuals with a legitimate business need to regularly access that area of the property and are pre-authorized by Community Security & Emergency Management Program Personnel to access those areas utilizing the access control system.

Security Alarm System: Device(s) intended to summon security and/or law enforcement personnel during, or as a result of, an alarm condition. Devices may include, but are not limited to, motion detectors, pressure switches, door/window sensors, glass break sensors, panic alarms, hold-up alarms, lockdown alarms, emergency exit alarms, software and other hardware.

Security Alarm Access Code: Code or phrase that is used by authorized individuals to arm, disarm, or activate a hold-up alarm or other devices using a security alarm system.

Tailgating: The act, either forced or accidental, of following an authorized user into an area that is normally secured by the access control system. This includes authorized personnel who neglect to tap their own access card when entering said area.

This policy applies to all Contractors of Community Transit, while on Community Transit property.

Visitors Note: Visitor policies and badges are covered in POL-SE-002 Visiting Community Transit Offices.

Section 1: Maintaining Access Control System Integrity

1. Public Area Entrances Unlocked During Normal Business Hours

In order to be welcoming and accessible for the public, public area entrances that are under the control of the access control system are unlocked during normal business hours. Security & Emergency Management Program personnel or first responders may direct doors to be locked during business hours. Public area entrances include the Ride Store Front Door and other locations as designed by the Manager of Security & Emergency Management or designee. Business Hours are generally defined as Monday through Friday 8am to 5pm, excluding major holidays. Specific hours may vary by location and business need.

2. Exterior Doors Stay Closed and Locked When Not Walking Through

All Exterior Doors remain closed and locked when an individual is not actively walking through, or moving items through, the doorway. This includes doors controlled by the access control system and doors not controlled by the system. Exterior entrances to public areas are exempt (Section 1.1).

3. Building Vehicle Bays Retain Ability to Be Locked

All exterior vehicle bays must have the ability to be locked with a physical locking mechanism or may have the power shut off using the access control system as a means of locking if there is a button on the exterior of the building that opens the bay without a key or access card.

4. Doors Controlled by Access Control System Stay Locked at all Times

Doors controlled by the access control system are to remain closed and locked at all times unless pre-approved by the Manager of Security & Emergency Management or designee.

5. Manager of Security & Emergency Management Manages the Access Control System

The Manager of Security & Emergency Management, or designee, pre-authorizes, in writing, any exterior doors and doors controlled by the access control system to be unlocked, locked, or to remain open unless otherwise approved in this policy. Authorized exceptions include, for example, conducting repairs while an employee stays next to the door while it is open or having an authorized vendor conduct repairs of a door or gate.

6. Unauthorized Access, Tampering or Bypassing Access Control System, Security Alarm System or Mechanical Key System is Prohibited

Tampering with or bypassing any component of the access control system or security alarm system is prohibited, Including, but not limited to:

- Damaging, disabling, vandalizing system(s).
- Unauthorized altering or modifying access software, system settings, devices, hardware, locks, keys or other access mechanisms.
- Propping doors or gates open to avoid the use of access devices or bypassing using a key, unless an exception to the policy has been authorized (Section 1.5).
- Admitting unauthorized person(s) into the building.
- Admitting an unauthorized a person through an access controlled door for which their access badge does not authorize them to have access unless they are being escorted the entire time by someone who does have access using the access control system.
- Utilizing a key to bypass an access control device, such as a card reader or emergency exit alarm.
- Utilizing an emergency exit for non-emergency use.
- Altering or counterfeiting access cards.
- Tailgating off of someone else's access card, including holding the door open for another individual to walk through without them scanning their badge on the card reader and the system indicating through a green indication light on access control system reader that they are appropriately authorized to enter using their badge.
- Utilizing a security access alarm code that is not assigned to the individual
- Altering or tampering with security signage unless authorized in writing by the Manager of Security & Emergency Management, or designee.

7. Individuals Should Question Persons without Badges

Individuals should request to see an access badge or visitor's badge of any person not wearing a valid access or visitor badge when in a non-public area, or report them to Community Transit Security & Emergency Management Program personnel.

8. Access Badges, Security Alarm Codes and Keys May Not Be Loaned or Used by A Person Other Than Bearer

9. Generic Access Badges and Security Alarm Codes Are Authorized on a Very Limited Basis

Generic access badges and security alarm codes, such as one that is provided to a vendor and shared among multiple individuals, must be pre-authorized by the Manager of Security & Emergency Management.

Examples include:

- Generic access badges for emergency use, or for temporary use by a current access badge holder while they locate their assigned badge.
- Generic codes for on-call emergency management and on-call facility emergency management.

Section 2: Accessing Community Transit Offices and Restricted Areas

1. Access to Community Transit Property

Individuals are welcome at Community Transit's property for the purposes of conducting Community Transit business, attending Community Transit events and activities, and when their attendance is requested by a Community Transit Contractor.

To maintain a secure environment, non-public areas and restricted areas of Community Transit offices are restricted to those individuals with a legitimate business need and who have the appropriate access level.

2. Individuals Follow all Community Transit Rules While On Property

Individuals are expected to follow all applicable Community Transit rules and posted signs during their visit, including all vehicle traffic control signs and security signs.

3. Access to Restricted Areas is Limited

Individuals are not to be given unescorted access to a Restricted Area if their Access Card does not allow access to that area. Individuals with a legitimate business need to occasionally access a restricted area must be escorted at all times by an individual whose Access Card provides regular access to that area.

Restricted Areas include the Cash Vault, Information Technology Server Rooms and Network Closet, Radio Dispatch, Ride Store Staff Areas, Kasch Park Casino Road (KPCR) Records Archive, Finance Secure Storage, Employee Engagement Secure Storage, Transit Security & Emergency Management Offices, Chief Executive Officer (CEO) Office and other areas designed with "Restricted Area" signage approved in-writing by the Manager of Security & Emergency Management. Access Card Readers to restricted areas generally utilize two factor authentication, such as a card reader with a PIN or a three factor, such as Card Reader with pin & biometric fingerprint reader.

Section 3: Access Badges & Keys

1. Access Badges Expire at Least Every 6 Years (effective January 1, 2023)

Access cards expire at the end of an individual's contract, term, or employment with an Authorized Contractor. All access badges expire at least every 6 years and must be replaced, including an updated picture. Replacement cards, due to expiration, are provided free of charge, provided the expired badge is turned in at the time of replacement. Individuals will receive a warning before badges expire. Individuals may not keep expired access badges after they are replaced.

2. Access Badge Photo Required

Access Badges are required to have a facial photo at the time of issue. Photos must contain the full front face of the individual, reflect the individual's current appearance, and cannot contain anything that covers the individuals face or head, unless otherwise approved for documented medical or religious reasons. Glasses with tint may not be worn in the photo.

3. Valid Government ID and Name Required

- The front of the Access Badges is required to have the individual's first name and first letter of last name, or preferred first name.
- The back of the Access Badge is required to have their legal name, as demonstrated by providing a valid government ID at the time of issuance of the badge.

4. Security & Emergency Management Program Personnel Issues New, Replacement and Temporary Access Badges

Security & Emergency Management Program personnel, or designees, issue new access badges.

Security & Emergency Management Program personnel, or designees, also issue replacement or temporary access badges for lost, stolen, damaged or worn-out badges.

5. Individuals Sign Rules of Use Form Prior to Receiving an Access Badge or Key

Individuals receive a copy of this policy and are required to read and sign a Rules of Use Form prior to receiving an access badge. The Rules of Use Form communicates policy compliance, the consequences for not following this policy, and the cost for lost Access Badges & Keys, including withholding of payments, as authorized (Section 3.12).

6. Individuals Receive an Access Badge Prior to Being Authorized in a Non-Public Area without an Escort or Visitor Badge

Individuals are required to receive an access badge or visitor badge prior to being in a non-public area without being escorted by an employee.

7. Individuals Access Our Buildings Using Their Access Badges

Individuals are required to use their access badge to gain entry to any door that is controlled by the access control system.

8. Individuals Wear Access Badges While On Community Transit Property Unless Otherwise Authorized

Individuals must prominently wear their access badge at all times while on Community Transit's property.

Access badges are authorized to be removed in certain situations:

- Individuals who drive Community Transit revenue vehicles are not required to wear their Access Badge while driving a Community Transit revenue vehicle, provided they are wearing an approved uniform.

- Individuals who work at Transit Centers & Park and Rides are not required to wear their Access Badge while at these facilities, provided they are wearing an approved uniform.

- Individuals doing job specific tasks in which wearing a lanyard may pose a safety risk, may wear an arm band badge holder instead of a lanyard in order to prominently wear their access badge in a safe manner. In the event this does not sufficiently mitigate the risk as determined by a job task hazard assessment conducted by the Risk Management Division, the arm band badge holder may be removed while performing the specific task as approved by Risk Management Division.

- **NOTE:** Individuals not wearing access badges, as outlined above, must have their access badge on their person, and must immediately produce the access badge if requested by an employee, board member, law enforcement or security & emergency management personnel.

9. Access Badges, Badge Holders/Lanyards & Keys are Returned to the Agency

Authorized contractors shall return their access badges, badge holders, lanyards and keys to their Community Transit representative on their last day of contracted work, or when requested.

Community Transit representative personnel shall promptly turn in access badges, holders, and lanyards to Security & Emergency Management Program personnel. Keys should be returned to the Facilities Maintenance Manager or designee.

10. Lost or Stolen Access Badges, Alarm Codes, or Keys Must Be Reported

Individuals must immediately report to Community Transit Security & Emergency Management Program personnel if their access badge, key or alarm code becomes lost or stolen by emailing Security.Info@commtrans.org.

11. Protecting Access Badges, Keys, and Alarm Codes

Individuals issued an access badge, key or alarm code has the responsibility to protect them and shall take all reasonable steps to ensure that items and information are safeguarded. Including, not leaving badges or keys or codes in:

- Unattended in open areas
- Inside of vehicles
- In areas where anyone else could use them

12. Fee Required for Lost, Stolen, Unreturned Access Badges or Keys

Individuals are required to pay an access badge / key fee to Community Transit for any access badge or key that is lost, stolen, or unreturned.

At the expiration and/or termination of a contractor's contract, final payment may be withheld until all contractor access badges & keys are returned to Community Transit Security & Emergency Management Program personnel. At the expiration and/or termination of a contractor's contract, all outstanding badge fees may be subtracted from final payment.

- **Fee Schedule:**
  - Contractor Non-Master Key / Access Badge: $100.00
  - Contractor Master Key or Grand Master Key: $5,000.00*

    *It should be noted that a lost Master Key or Grand Master Key may result in having to re-key all locks and therefore can cost $30,000, or more, to mitigate.

13. Access Levels Changes and Forfeiture of Badge / Key May Be Required for Security & Safety Concerns

Individuals who are subject to disciplinary action, workplace investigations, or investigational leave, may have their access levels modified or access badge / key forfeited due to security or safety concerns, at the discretion of Security & Emergency Management Program personnel.

14. Access Badges Are Not Bus Passes

Access badges do not function as a bus pass on any transit system.

Section 4: Access Policy Administration and Enforcement

1. Community Transit's Manager of Security & Emergency Management, or designee, administers and enforces the access policy for the agency:

- Approves agency-wide badge designs, holders and lanyards.
- Develops agency-wide forms, procedures and tasks for the implementation of this policy.
- Develops agency-wide access levels, including hours of operations, for the implementation of this policy.
- Approves all new access control systems and modifications to existing systems, including changes to hardware, software, equipment, programming and installation specifications.
- Approves all new security alarm systems and modifications to existing systems, including changes to hardware, software, equipment and installation specifications.
- Approves exception to this policy, for the purpose of conducting repairs or maintenance.
- Approves exception to this policy, for the purpose of facilitating major capital projects.
- Authorizes designation of "Restricted Areas" in consultation with manager who oversees the operations of the areas in question.
- Approves the hardware, including lock type, used for the mechanical key system.
- Develops agency-wide key access levels for the implementation of this policy.
- Conduct audits to ensure compliance with this policy
- Acts as an authorized agent of Community Transit for the purpose of notifying an authorized contractor to vacate Community Transit's offices or be subject to exclusion and/or criminal trespass for violations of this policy, other company policies or rules, or applicable laws.

2. The Facility Maintenance Administers the Mechanical Key System:

The mechanical key system, including physical locks and keys, is administered by the Facility Maintenance Division, as authorized by the Security & Emergency Management Program personnel. This includes issuing keys as authorized by the Security & Emergency Management Program.

- Security & Emergency Management Program personnel, or delegates, authorize issuing of new keys or modification of an individual's key levels
- Restroom Keys are administered by the Transportation Department & Facility Maintenance Division as authorized by the Security & Emergency Management Program personnel.

3. Authorized Contractors May Be Escorted from the Premises or Excluded

While visiting Community Transit's office, authorized contractors are expected to follow Community Transit's rules and posted signs. Failure to do so could result in a request to leave and/or being escorted off the premises by Community Transit's Manager of Security & Emergency Management or designee. In some cases, depending on the severity of the situation and concerns for safety and security, persons could be excluded from Community Transit property and subject to criminal trespass for violations of a notice of exclusion.

Approved by: Ric Ilgenfritz

Ric Ilgenfritz, CEO

Written by:
Jacob Peltier, Manager of Security & Emergency Management
Becky Gibler, Assistant Manager of Security Operations

Cancels or supersedes:
166-POL-001 Using Community Transit Photo ID Badges - June 5, 2005
166-POL-005 Badges for Board Members and Their - June 5, 2003
Board Resolution No. 9-03
Board Resolution No. 10-03

Last reviewed:
Reviewed by Policy Committee Team April 29, 2021

See also:
POL-SE-0002 Visiting Community Transit Offices

Washington Office of Secretary of State - Local Government Common Records Retention Schedule (CORE) Version 4.0 (May 2017)

- GS50-06B-05 Rev. 1 – Inventory Keys/ Key Cards / Badges
- GS50-06B-20 Rev. 1 – Security Monitoring – Employee and Public Access

RCW 9a.52 – Burglary and Trespass