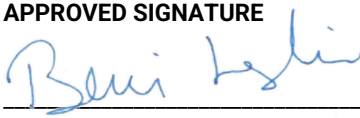


 STATEWIDE POLICY	NUMBER 107-011-170	SUPERSEDES Policy #107-011-170 (2003)	
	EFFECTIVE DATE June 10, 2025	PAGE NUMBER Pages 1 of 6	
	LAST REVIEWED DATE June 10, 2025		
	REFERENCE/AUTHORITY ORS 276.021, 276.210 and other related provisions of ORS chapter 276		
DIVISION Enterprise Asset Management	APPROVED SIGNATURE  Berri Leslie, DAS Director		
POLICY OWNER Facilities			
SUBJECT Building Security Access			

PURPOSE

To guide the process of issuing keys, keycards, photo IDs and temporary key or keycards for the Building Security Access Unit.

APPLICABILITY

All state agency officials, employees or other holders of keys, keycards or a photo ID allowing access to a facility owned, managed or leased by DAS.

FORMS/EXHIBITS/INSTRUCTIONS

- High-Security Access Area Request form (request from Building Security Unit)
- Keycard, Key, and Photo ID Coordinator Signature Authorization form (request from Building Security Unit)
- Project Authorization Request form
- Price List of Goods and Services

DEFINITIONS

Agency: The state agency that occupies or controls a building owned by the Department of Administrative Services (DAS).

Building Security Unit: The unit within DAS that is responsible for keys, keycards, photo IDs and the access control system. Contact:

Department of Administration Services, EAM Building Security Unit
 1257 Ferry Street, SE, Salem, Oregon 97310
 Phone: 503-373-7001 or 503-373-7025; 503-378-2759 (fax)
 Email: FacilitiesDAS.KeyCardSalem@das.oregon.gov

Controlled access building: A general security classification given to state buildings. All facilities owned, managed or leased by DAS are considered controlled access buildings requiring keycards to be issued to authorized personnel.

Coordinator: Employee assigned by an agency to approve and process issuing keys, keycards or photo IDs.

Division: Department of Administrative Services, Enterprise Asset Management, Building Security Unit.

High-security access area: An area that requires a higher level of controlled access. Area is limited to authorized personnel only, may include employees authorized by the employer and required by work duties to be present in the regulated area; any person entering the area as a designated representative for the purpose of exercising the right to monitor procedures; and a competent person authorized for construction activities using appropriate safety control protocols.

High-security area representative: Employee assigned by an agency head to approve access to high-security access area(s).

Key: A notched metal device used to open mechanical hardware on doors.

Keycard or card: Programmable electronic “keys” which allow users to enter secured buildings or rooms during set times.

Keycard or key coordinator: Employee assigned by an agency to approve issuance and deactivation of keys, keycards or photo IDs and maintain all associated records. This employee also requests any modifications to keycard reader programming.

Keycard readers: Electronic devices, which read encoded electronic identification on keycards and allows authorized cardholders access to a building or space.

Keycard shop: Informal name used by an agency employee when referring to DAS-EAM, Building Security Unit.

Photo ID: A keycard or photo ID with the photo of the authorized cardholder on the face of the card.

Project authorization: A review and approval procedure for all remodeling projects, including the installation of keyed locks or keycard readers, for facilities owned, managed or leased by DAS. Submit a [Project Authorization Request](#) form.

Representative: Employee assigned by agency to approve the issuance of keys, keycards, or photo IDs to high-security access areas.

Temporary key or keycard: Key or keycard issued to keycard coordinators for use in special cases requiring short term access.

TRIRIGA software: The division’s facility management software is used to track agency requests.

TRIRIGA team: DAS EAM employee to contact regarding software issues and training on TRIRIGA software functions. Contact: TRIRIGA.Needs@das.oregon.gov

EXCLUSIONS AND SPECIAL SITUATIONS

- To make an exception to this policy, the agency must submit a written request to: FacilitiesDAS.KeyCardSalem@das.oregon.gov. The requesting agency must affirm it has met all their internal agency policies and the request must be approved by the DAS-EAM administrator or designee.
- All keycard readers, including high-security access area keycard readers, are added to state police, fire department and building emergency access.

GENERAL INFORMATION

(1) Controlled access building or areas

- a) **Costs of security.** The Building Security Unit installs keycard readers and keyed locks on essential doors and elevators in the buildings DAS owns or operates, as agreed to in lease negotiations. Agencies may request additional keycard readers, locks or other security equipment required to enhance safety and security. The costs of installation, on-going maintenance, repair and replacement, keying changes and all costs to convert back to original hardware is the responsibility of the requesting agency. Hourly rates are referenced in the Price List. Prior approval by the DAS Project Authorization Committee is required by submitting a Project Authorization form. The committee considers building security, fire and life safety, cost effectiveness and the needs of other tenants.
- b) **Employee responsibilities.** Keys, keycards and photo ID are the property of the State of Oregon, subject to the authorizing agency's control. Employees must return keys, keycards, and photo ID upon deactivation of access or termination of employment. Keys, keycards and photo IDs must be issued, controlled and used as described in this policy. An individual violates this policy when using or holding a key, keycard, or photo ID that was not assigned to them. No individual shall use a key, keycard, or photo ID to give access to someone who does not have the authority to be in the controlled space or High Security Access Area . No individual may load or re-assign their key, keycard, or photo ID to another individual. Lost keys or keycards must be reported to your supervisor or key coordinator immediately. Loss of assigned keys or keycards will result in rekeying costs. Replacement keycard rates include the direct costs of supplies, equipment and labor used to produce each card. Should a lost or stolen key, keycard or photo ID be recovered, it cannot be re-activated due to security risks and must be returned to DAS immediately. Refusal to return a key or keycard may result in the employer pursuing legal remedies to recover the cost of re-keying. Oregon law does not permit withholding pay from final paychecks for failure to return key or keycard (employer property). Oregon law [ORS 652.610\(3\)](#) prohibits deductions from wages unless they are required by law, voluntarily authorized in writing by the employee, authorized by a collective bargaining agreement, or made upon termination of employment.

(2) Agency responsibilities

- a) Each agency must name a coordinator and one or more alternates. To add or remove a coordinator, the agency requests a Keycard Coordinator Authorization form from the Building Security Unit and returns the completed form, which must include the agency head's signature. It is recommended to have a human resource employee listed as one of the alternate coordinators, and keep the signature forms up to date. A new form supersedes all previous assignments, and the new coordinator assumes responsibility for the items on the signature form.
- b) In cases requiring a security background check, the requesting agency completes the appropriate security background check prior to requesting a keycard.

- c) The coordinator for an agency requesting a high-security access area must request a high-security access area form from the Building Security Unit, which when submitted, will be reviewed by the division administrator (or designee) for approval.
- d) Each agency with a high-security access area must name a representative and one or more alternates who will have the authority to approve access to the area. To add or remove a representative, the agency requests a High-Security Signature Authorization form from the Building Security Unit and returns the completed form, which must include the agency head's signature.
 - The role of the representative is distinct from a coordinator's role. High-security access area representatives focus on authorizing who has access to high-security access areas. Agency coordinators submit requests to the Building Security Unit and manage distribution of keys, keycards, and photo IDs.

(3) Division administrator's responsibilities

- a) The division administrator, deputy administrator, or a designee appointed in writing, may authorize keys, or keycards for access to areas owned or serviced by DAS, as necessary for any employee's work, unless designated as a high-security access area. At the administrator's discretion, access to certain areas requires that the potential cardholder undergo a criminal background check and be approved by Oregon State Police or others before a key or keycard will be issued or continued.
- b) The division administrator, deputy administrator, or a designee appointed in writing, reviews and approves requests for any new high-security access areas.
- c) When a building area has been modified or newly designated as a high-security access area, there may be existing keys or keycards that allow access to the area. Upon approval of the high-security access area request by the division administrator, deputy administrator, or a designee appointed in writing, the coordinator requests a report of who has access to the area through a TRIRIGA request. The Building Security Unit will work with the coordinator to facilitate the high-security access area request.

(4) Keycard coordinator roles and responsibilities

- a) After the approval of a Keycard Coordinator Authorization Signature form, the Building Security Unit will let the Coordinator know that TRIRIGA.Needs@das.oregon.gov will be contacting the coordinator regarding setting up a TRIRIGA account and provide them with some additional information. Coordinators must safeguard their access to TRIRIGA and ensure all requests from their agency have been properly authorized and submitted to a Keycard or key coordinator. The division is not responsible for unauthorized requests.
- b) The coordinator keeps records of all keys, keycards, and photo IDs that they authorize. In addition, coordinators must keep records of all access levels they are responsible for and are authorized to assign, including access levels assigned to other agency's cards. Building Security Unit personnel do not select the access levels to be assigned to cardholders; Coordinators submit requests through TRIRIGA software, and the Building Security Unit facilitates those requests.
- c) Coordinators may approve keys, keycards, or photo IDs only for buildings in which their agency is a tenant or owner. In those buildings, a coordinator may approve access to the internal space their agency rents or owns, and to shared or common areas. Common areas include building entries and hallways, conference rooms, or other areas that the owner and tenant all agree to share. Exceptions to a coordinator's authority may be granted by the division administrator or division designee in writing.

- d) Coordinators may also authorize changes to the times the doors lock and unlock in the areas under their authority by emailing the request to the Building Security Unit. Exterior entry door or reader unlock times also require the approval of the division. Coordinators are responsible for obtaining the approval of all tenant and owner agencies involved.
- e) Coordinators must always keep all keys and keycards under their immediate control, including deactivated items waiting to be returned to the Building Security Unit. Any keycard returned to the Building Security Unit by mail must be deactivated first. Coordinators must return all keys, keycards or photo IDs as soon as items are no longer needed.
- f) Coordinators may submit an employee's photo by attaching the .jpg photo to the TRIRIGA request.
- g) Coordinators use TRIRIGA software to request keys, keycards or photo IDs for employees and to authorize changes to existing keys or keycards (activate or deactivate, modify and replace lost or damaged cards). A coordinator's approval submitted through a TRIRIGA request represents to the division that all the agency's internal policies have been met and all information in the request is correct.
- h) Each TRIRIGA request may have an associated cost, which is the responsibility of the requesting agency. The Building Security Unit's fees for keys, keycards and photo IDs depends on the type of item requested by the agency. An agency may choose cards with or without photos. For pricing details consult the Price List of Goods and Services or contact the Building Security Unit. Once cards are issued, the agency pays all costs to convert to another card type.
- i) Completed key cards are shuttled over to the employee's primary place of employment, then the coordinators distribute them to employee. In special circumstances, coordinators or the employee who the card is being issued for, may pick up key cards at the Building Security Unit by making an appointment.
- j) Coordinators must immediately notify the Building Security Unit personnel by phone if a key or keycard has been lost, stolen or requires immediate cancellation or modification. In addition, Coordinators must follow up with a TRIRIGA request to deactivate key or keycard.
- k) In special cases, the Building Security Unit may issue a Temporary Key or Keycard to a Coordinator, or an employee authorized by the coordinator. The coordinator or authorized employee may then issue the Key or Keycard to a temporary user such as a construction vendor to perform a repair or a temporary business partner or vendor performing a specific project for a limited period of time. The user of a Temporary Key or Keycard has full responsibility for it and its use and must follow the expectations outlined in "Employee Responsibilities" Section 1 (b).
- l) Coordinators should request reports through TRIRIGA to assist with recordkeeping.
- m) Agency management must notify the Building Security Unit as soon as possible and preferably at least one week prior to the employee in the role of coordinator being vacated. An existing coordinator must provide a current inventory to a new replacement. The new coordinator assumes responsibility for all keys and keycards issued by the previous coordinator.

(5) Building security unit's roles and responsibilities

- a) It provides keys, keycards, photo IDs and access control related services, and completes special security projects requested by agencies and approved by the division, according to the terms of agreement.
- b) It helps with entering Building Security Unit TRIRIGA requests.
- c) It does not assume liability for unauthorized access to controlled access areas, including high-security access areas. When a coordinator submits a request through TRIRIGA for access to a high-security access area, they need to have already obtained the approval of their agency's high-security area representative. This approval does not go to the Building Security Unit. Rather, its purpose is to satisfy each agency's need to control access to an area and to maintain proper records.
- d) It provides reports upon request through TRIRIGA. Examples are as follows:
 - (A) The names of valid keycard holders.
 - (B) Activity on a keycard or keycard Reader.
 - (C) The names of keycard holders who have access to a high-security access area.
- e) To the extent permitted by law, photos taken of keycard holders must be used for state identification only.
- f) It reserves the right to deactivate keycards at any time to address security risks. Keycard or Key Coordinator and High Security Area Representatives will be notified immediately of any deactivations. Coordinators must follow up with a TRIRIGA request to deactivate key or keycard.
- g) In the event of an emergency when the building is facing an imminent security threat and needs to be put on high alert or lock down, building emergency coordinators will direct emergency protocols established for the building. For additional information view the State of Oregon Comprehensive Emergency Management Plan (CEMP) prepared by the Oregon Emergency Management Department. This document combines a number of documents into a single plan covering four mission areas of emergency management include Mitigation, Preparedness, Response and Recovery. Other guidance can be found in Guidelines for Suspicious Mail.