THE OHIO STATE UNIVERSITY

Physical Access Management and Control

University Policy

Applies to: Employees, students, volunteers, guests, contractors, and authorized vendors

Responsible Office — **Office of Administration and Planning**

POLICY

Issued: 04/27/2021

The university is committed to providing a safe and secure physical environment and appropriate control of access to university assets and data. The university's physical environment includes hundreds of **facilities** and thousands of rooms, many of which require controlled access to help ensure the safety of university community members and the security of university property. This policy covers all university facilities; all keys, cards, and other devices that control access to university facilities; and all individuals granted access permission to university facilities.

Purpose of the Policy

To establish a comprehensive and coordinated **physical access control** management process across the university enterprise.

Definitions

Term	Definition
Access reader	Typically, a wall or door-mounted reader that connects to the physical access control system.
Authorized key signer	An individual responsible for issuing, receiving, and maintaining key assignments, key inventories, transaction systems, forms, and records as delegated by unit leaders or their designees.
Building construction project	Refer to the Building Design Standards for the most up-to-date definition.
Delegate administrative area	Administrative area responsible for the oversight of approved physical access control systems. A complete list of delegate administrative areas can be found on the Physical Access Management webpage.
Employees	Faculty, staff, student employees, and graduate associates.
Facilities	All buildings and other physical structures owned, rented, or leased by the university, including The Ohio State University Wexner Medical Center.
Master keys	A key that provides access to more than one space. There are several levels of master key, each with different capabilities and rules for issuance and use (e.g., master key, sub-master key, multiple cores).
Monitoring	Identifying and recording cardholder information and logging system events.
Physical access control	Assignment of permissions to authorized individuals and management of physical access to buildings, rooms, and physical assets
Physical access control system	A coordinated and centrally managed mechanical and/or electronic group of devices used to physically secure buildings, rooms, and physical assets. Devices include but are not limited to physical keys; key fobs; keypads; card readers; biometric readers; combination locks; lock boxes; electronic key cabinets; lock cylinders; automatic door operators, closers, and hinges; radio-frequency identification (RFID); or any combination of devices used to control access. Devices do not include the doors themselves.
Physical access points	A controlled threshold into a physical space.
Physical access system	A defined structure used to manage physical access to buildings, rooms, and physical assets across campus.
Physical access types	Permission sets that allow access to buildings, rooms, and physical assets as defined by the responsible administrative unit.

Applies to: Employees, students, volunteers, guests, contractors, and authorized vendors

Term	Definition
Program of requirements	Information that outlines the scope of the construction/renovation project from the using agency and the detail requirements needed for that space(s) as described in the Building Design Standards.
Restricted access space	Physical space that due to the nature, use and/or physical assets contained therein requires a higher level of security (e.g., high voltage spaces, roofs/tunnels, or confined spaces).
The Ohio State University Wexner Medical Center (Ohio State Wexner Medical Center)	University Hospital, East Hospital, Brain and Spine Hospital, Richard M. Ross Heart Hospital, Harding Hospital, Dodd Rehabilitation Hospital, Ambulatory Clinics and Services, and Arthur G. James Cancer Hospital and Richard J. Solove Research Institute and Outreach Sites; College of Medicine and its School of Health and Rehabilitation Sciences; the Office of Health Sciences, including OSU Faculty Group Practice; various research centers, programs, and institutes; and The Ohio State University Comprehensive Cancer Center.
Unit	College or administrative unit.
Unit leader	Head of college or administrative unit (e.g., dean, senior vice president, president, provost).
University-issued ID card/badge	A physical or digital credential issued by the university to identify the holder and their affiliation and role with the university. May also be used as an access control device for an electronic access control system.
University-issued keys	Any physical key (often referred to as a “brass key”) that is issued by the university.

Policy Details

I. Overview

A. The Ohio State University is committed to providing a safe and secure environment in all of its facilities. This includes but is not limited to the selection, installation, and management of **physical access control systems** and the administration of physical access into university facility spaces.

B. Leased or rented properties are required to adhere to this policy when use of those properties includes the selection, installation, and/or management of physical access control systems.

C. Any buildings in existence prior to the issuance date of this policy will not be required to conform to this policy until renovation work is undertaken and/or at the request and direction of a **unit leader**.

D. Costs entailed to meet the requirements of the policy are the responsibility of the **unit**.

II. Applicable Principles

A. Securing access of the university’s physical spaces will be managed in a way that supports the university’s current Framework Plan and the additional objectives of:

1. Supporting teaching, learning and research;
2. Providing accessibility to a broad cross-section of the population;
3. Controlling access by incorporating access control best practices;
4. Balancing initial and long-term operating costs; and
5. Complying with external laws and regulations and other university policies.

B. The above objectives and this policy’s requirements must be considered in the design of all qualifying **building construction projects**.

C. **University-issued keys** and/or **university-issued ID card/badges** become the individual’s responsibility until termination of employment, separation from the university, or the granted access to a space(s) is no longer needed.

1. Delegate administrative areas are responsible for the management of the return, proper documentation, and transfer of university-issued keys and/or ID card/badges.

D. Keys and ID card/badge access are assigned to individuals and may not be passed along to any other personnel.

1. If the space requires key and/or ID card/badge access, individuals should not let an unauthorized person follow into the secure area.

E. The university is committed to maintaining a high level of security for access control while allowing appropriate levels of access for employees, students, volunteers, guests, contractors, and authorized vendors.

III. Physical Access Control of Facilities

A. Authorization for access to a physical space is determined by:
   1. Business purpose of the space;
   2. Mandatory requirements (e.g., Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) Requirements, Information Security Control Requirements (ISCR)); and
   3. The role the individual has within the organization.

B. **Physical access types** are utilized to assign those space(s) an individual receives access to, based upon the above considerations and the requirements outlined in the Physical Access Type Considerations document.

C. **Delegate administrative areas** must use the Physical Access Type Consideration document to assign the appropriate access types.

D. Units must ensure that the access permissions they manage are reviewed down to the individual level at least annually for university-issued keys and university-issued ID cards/badges that grant access to physical spaces. More frequent reviews should be conducted when the physical space(s) is subject to:
   1. A change in space use;
   2. A change in an individual access holder’s role;
   3. A loss of university-issued key, university-issued ID card/badge, and/or credential granting access to a space;
   4. High turnover or frequent access changes due to the nature of the space;
   5. High risk as determined by the delegate administrative area; and/or
   6. Internal or external mandates or identified security needs that set those review requirements.

IV. Physical Access Systems for Facilities

A. All units are required to follow applicable Building Design Standards (BDS) on **physical access systems**.

B. Only approved physical access control systems identified in the BDS may be installed on university facilities, and units must ensure the following requirements are met.
   1. Exterior doors
      a. A minimum of one exterior door must be designated as a 24/7 access point for use as determined in the design process for the building. That entrance must be electronically controlled, be ADA compliant, report to a delegate administrative area for **monitoring**, and have an **access reader** for after-hours building access.
      b. Any door that will be open to the public during operating hours must be electronically controlled and connected to an approved access control system for monitoring.
      c. All exterior doors deemed exit-only and controlled by university-issued key access must remain locked from the outside at all times. Building occupants are required to ensure that these doors are not be propped open unless supervised by authorized personnel.
      d. University-issued keys that provide access to exterior doors may not be issued to building occupants.
      e. Exceptions may be requested for buildings with a high volume of traffic and transient occupancy (e.g., classroom buildings, dining facilities, and libraries) as determined during the building design process.
   2. Interior doors
      a. The selection of the appropriate system will be determined by the delegate administrative area, and reported to Physical Access Shared Services (PASS) in the Office of Administration and Planning, based on space use and the users of the space.

   b. If there is a space use change and/or a space reassignment, the incoming unit must work with their delegate administrative area to evaluate the space to ensure the appropriate system is installed and reported to PASS.

3. Approved electronic physical access control systems must:
   a. Provide for central monitoring ability by a delegate administrative area;
   b. Provide for central control (the ability to schedule automated locking and unlocking and to lock and unlock on demand from a remote location); and
   c. Maintain a physical key override for emergency access in the event of a system failure.
4. No off-line electronic readers will be permitted for use in physical access control systems.

C. For reasons of safety and design, locking mechanisms may not be altered, added, or removed by end users. Unauthorized duplication, modification, or reproduction of any university-issued key or ID cards/badges is prohibited (See Faculty Rule 3335-13-04).

V. Governance

A. Physical Access Shared Services (PASS) in Administration and Planning
1. PASS reports to the office of the senior vice president of administration and planning.
2. PASS will coordinate with all delegate administrative areas that maintain approved physical access control systems and their system administrators to ensure policy compliance and compatibility across the enterprise.

B. Physical Access Management and Control Steering Committee
1. The Physical Access Management and Control Steering Committee (Steering Committee) serves as a governance committee for physical access management.
2. The Steering Committee reports to the senior vice president of administration and planning.
3. Steering Committee membership consists of representatives from Athletics, Department of Public Safety, Facilities Operations and Development (FOD), Office of the Chief Information Officer (OCIO) Enterprise Security Team, Student Life, Medical Center Security, and others identified and appointed by the senior vice president of administration and planning.
4. PASS chairs and convenes the Steering Committee.
5. Steering Committee responsibilities are defined in the committee charge.

C. Senior vice president of administration and planning
1. The senior vice president of administration and planning is responsible for the administrative oversight of PASS and ensuring the appropriate processes are followed for the removal, addition, or change of physical access systems for facilities.

D. Delegate Administrative Areas
1. Each delegate administrative area will:
   a. Provide oversight for approved physical access control systems within their areas; and
   b. Ensure and report policy compliance to PASS.

E. Exception Requests
1. In rare circumstances, units may contact PASS to discuss alternatives or the need for a possible exception to the university-approved physical access control systems or this policy.
2. If an alternative cannot be found, the unit leader or their designee may submit an exception request to PASS.
3. Approved exceptions apply only to the specific circumstances/areas covered by the request and do not provide blanket exceptions for future similar use cases. However, exception requests for a grouping of like spaces may be submitted at the same time.
4. All exception requests will be reviewed by the delegate administrative area, PASS, and the Steering Committee.

5. Exceptions to the university approved physical access control systems and/or this policy require the approval of the senior vice president of administration and planning or their designee prior to implementation.

PROCEDURE

Issued: 04/27/2021

I. Physical Access Control System Selection
   A. As part of the construction/renovation process, the **program of requirements**, which occurs at the very beginning of the design process, will be used to identify the appropriate physical access system controls to be installed on all **physical access points** within the project.
   B. Determination for the physical access control system will consider the following parameters, including but not limited to whether the space:
      1. Has access to intellectual property or other sensitive information;
      2. Has access to legally protected data as defined by the Institutional Data policy;
      3. Has access to cash or credit card information;
      4. Has items in the space that represent a theft risk;
      5. Has access to student and/or protected health information;
      6. Is a residential living space;
      7. Has access to IT infrastructure;
      8. Has access to critical maintenance or is designated as **restricted access space** (e.g., high voltage spaces, roofs/tunnels, or access to confined spaces); and/or
      9. Has external mandates or identified security needs that sets those access requirements.
   C. When determining which system/hardware to install, units must work with the appropriate delegate administrative area to advise and inform the selection of the appropriate system/hardware.

II. University-Issued ID Cards/Badges
   A. The university recognizes the BuckID card as the only official identification cards to be utilized to obtain access to facilities.
      1. Additional identification badges will not be encoded for access control purposes.
   B. Loss of university-issued ID cards/badges
      1. Individuals must report loss of a university-issued ID card/badge to the appropriate system administrator immediately.
         a. For BuckID cards, follow the steps outlined on the BuckID website for lost or stolen cards.
         b. For Ohio State Wexner Medical Center ID cards, contact Medical Center Security.
      2. Electronic access will be suspended immediately upon notification. Access will be reinstated automatically when a replacement ID card/badge is issued.

III. University-Issued Keys
   A. University-issued keys provide a means to access an assigned space based upon an individual's role within the organization.
      1. Individuals must return all access keys to the university immediately upon:
         a. Termination and/or separation from the university; or
         b. A change in their role that ends their need to access the space.
   B. **Master keys** provide a means to access multiple spaces and provide operational efficiencies but create opportunity for broad compromise exposure. Generally, building master keys will not be issued. To further mitigate potential exposure, units must adhere to the following:

1. Approved access to master keys is role-based as outlined in the Physical Access Type Considerations document. Requests for additional access must be submitted by **authorized key signers** through the delegate administrative area.
2. Master keys must remain on campus at all times.
3. Master keys, when not in use, must be stored in electronic key cabinets.

C. Restricted access keys provide an additional level of access control to restricted access spaces. The distribution of these keys should be very limited and must adhere to the following:

1. Restricted access keys can only be carried by university employees.
2. Restricted access keys and locks require approval by the **unit leader,** delegate administrative area, and PASS.

D. Loss of University-Issued Keys

1. Individuals must report a lost or compromised university-issued key immediately 24/7 to their supervisor (if employed by the university) and to one of the following:
   a. Service to Facilities (S2F) at 614-292-4357 for lost or compromised keys in all units except the Ohio State Wexner Medical Center; or
   b. Medical Center Security at 614-293-8500 for lost or compromised keys in the Ohio State Wexner Medical Center.
2. The delegate administrative area, in consultation with the unit that lost the key, will recommend the necessary risk exposure mitigation steps and report those to PASS for review and approval.
3. If a key is lost, stolen, or not returned by an individual upon separation from the unit/university, the unit or contractor/vendor is responsible for all costs incurred to mitigate exposure due to the key loss. This may include but is not limited to the access control device replacement, including mechanical keys and required "re-keying" of locks due to the loss of an access control device by their device holder, as well as security services needed to mitigate the risk of the loss.
4. Any key(s) found by a person other than the assigned key holder should be immediately returned to the Ohio Union Lost and Found or to the Medical Center Security.

IV. Exception Request Process

A. Only unit leaders or their designees may request an exception to any requirements of this policy.

1. Exception requests regarding physical access systems for facilities are submitted using the Physical Access Systems Exception Request Form.
2. Exception requests regarding university-ID cards/badges and university-issued keys are submitted using the Card and Key Exception Request Form.

B. All exception requests and compelling documentation as to the business reason for the request must be submitted for consideration prior to entering or during the program of requirements phase for facilities.

C. The delegate administrative area and PASS, in consultation with the Steering Committee, will review each timely exception request. The Steering Committee will then make a recommendation to the senior vice president of administration and planning for final review.

D. All exception requests require approval by the senior vice president of administration and planning or their designee prior to implementation of the exception.

V. The university may enforce corrective action, up to and including termination, in accordance with applicable policies or rules for violations of this policy.

Responsibilities

Position or Office	Responsibilities
Authorized key signer	Submit requests for additional access through the delegate administrative area.

Applies to: Employees, students, volunteers, guests, contractors, and authorized vendors

Position or Office	Responsibilities
Delegate administrative areas	1. Provide oversight for approved physical access control systems within their areas as set forth in the policy. 2. Ensure and report policy compliance to PASS. 3. Review exception requests in consultation with PASS and Steering Committee. 4. Consult with units to recommend appropriate risk mitigation steps for lost university-issued keys to PASS. 5. Approve requests for restricted access and locks as appropriate.
Physical Access Management and Control Steering Committee	1. Serve as governance committee for physical access management. 2. Reviews exception requests in consultation with delegate administrative areas and PASS and make recommendations to SVP of administration and planning for final review.
Physical Access Shared Services (PASS)	1. Coordinates with delegate administrative areas to ensure policy compliance as set forth in the policy. 2. Chairs and convenes Steering Committee. 3. Review and approve recommended risk mitigation steps for lost university-issued keys. 4. Reviews exception requests in consultation with the delegate administrative areas and Steering Committee. 5. Approve requests for restricted access and locks as appropriate.
Senior vice president of administration & planning	1. Provides administrative oversight of PASS. 2. Ensures appropriate processes are followed for physical access systems. 3. Considers and rules on all exception requests.
Space user (ID Card/Badge and University-Issued Keys)	1. Responsible for all university-issued keys and ID card/badges as set forth in the policy. 2. Return issued keys upon termination or separation from the university or when there is a change in their role that ends their need to access that space. 3. Report lost or compromised keys immediately 24/7 as set forth in the policy. 4. Report any key found immediately to Ohio Union Lost and Found or to Medical Center Security.
Units	1. Follow applicable Building Design Standards on physical access systems as set forth in the policy. 2. Review access permissions down to the individual level at least annually for university-issued keys and university-issued ID cards/badges that grant access to physical spaces. 3. Consult with delegate administrative areas to recommend appropriate risk mitigation steps for lost university-issued keys to PASS. 4. Ensure compliance with the policy within their unit.
Unit leaders	1. Submit any policy exception requests. 2. Approve requests for restricted access and locks as appropriate.

Resources

Forms

Physical Access Systems Exception Request Form, go.osu.edu/accessexception
Card and Key Exception Request Form, go.osu.edu/cardkeyexception

Governance Documents

Building Design Standards, fod.osu.edu/bds
Institutional Data Policy, it.osu.edu/sites/default/files/files-1477502242/institutionaldata.pdf
Information Security Control Requirements (ISCR), go.osu.edu/infosec-iscr
Information Security Standard (ISS), go.osu.edu/infosec-iss
Payment Card Industry Requirements, busfin.osu.edu/sites/default/files/quick-start-guide-pci-requirements.pdf
Rules of the University Faculty, 3335-5-04, trustees.osu.edu/university-faculty-rules/3335-13

Websites/Additional Guidance

BuckID, buckid.osu.edu/
Department of Public Safety, dps.osu.edu/about
Facilities Operations and Development, Lock & Key Services, fod.osu.edu/

Family Educational Rights and Privacy Act (FERPA), ed.gov/policy/gen/guid/fpco/ferpa/index.html
Health Insurance Portability and Accountability Act (HIPAA), hhs.gov/hipaa/index.html
Physical Access Management Webpage, fod.osu.edu/pam
Physical Access Type Considerations, ap.osu.edu/sites/default/files/physical_access_type.pdf

Contacts

Subject	Office	Telephone	E-mail/URL
Building Design Standards	Design & Construction	614-292-4458	https://fod.osu.edu/about/design-and-construction
Delegate administrative area for Athletics	Fawcett Center for Tomorrow	614-292-6330	ath-accesscontrol@osu.edu
Delegate administrative area for CFAES Wooster	Safety and Compliance	330-263-3665	CFAESAccessmanagement@osu.edu https://cfaessafety.osu.edu/
Delegate administrative area for Facilities Operations and Development	Lock & Key Services	614-292-1415	key-control@osu.edu (for brass keys) key-card@osu.edu (for card access)
Delegate administrative area for Student Life	Risk and Emergency Management; BuckID	614-292-4357	Go.osu.edu/ekey Buckid.osu.edu
Delegate administrative area for the Ohio State University Wexner Medical Center	Medical Center Security	614-293-8500	Security Managers@osumc.edu
General policy questions	Administration and Planning	614-292-3080	ap.osu.edu
Reporting lost or compromised keys 24/7	Service2Facilities Medical Center Security	614-292-4357 614-293-8500	fod.osu.edu/make-request Security Managers@osumc.edu

History

Issued:	04/27/2021
Edited:	05/03/2021