Ohio Administrative Code

Rule 3337-44-50 Physical Access Control.

Effective: December 19, 2018

The version of this rule that includes live linksto associated resources is online at

https://www.ohio.edu/policy44-050.html

(A) Overview

This policy establishes appropriate access control standards and procedures to enhance the physical security of Ohio university facilities and assets.

Ohio university access control is the functional area designated to maintain appropriate facility access control systems and procedures to enhance the safety and security of Ohio university students, employees, contractors, vendors, guests, assets, research, and records.

To this end, the university access control office and the university lock shop have the sole authority to install, manage, maintain, modify, and operate all facility access control systems on the Athens campus. This includes both physical key and electronic access control systems. Electronic access control system are maintained and operated in partnership with the office of information technology. These functions may be delegated to other appropriate personnel at Ohio university regional campuses, extension campuses, and centers at the discretion of the vice president for finance and administration.

Ohio university requires that departments and units maintain appropriate records and control of all keys and access credentials issued to them by access control in compliance with the provisions defined below. In addition, individual key and credential holders also have personal responsibilities related to use, protection and disposition of university keys and access credentials.

(B) Principles

Issuance of keys and access control credentials should be evaluated on a case-by-case basis. Keys and credentials should be issued only when necessary, especially when granting access to space that contains valuables, confidential materials, dangerous substances, or equipment.

The following principles should be applied in determining if issuance of a key or credential is warranted:

(1) Alternative access

Whenever possible, utilize means for access that do not require the issuance of keys or credentials to an individual especially when the need for access is infrequent, arises because of special circumstances, or is short-term. In such circumstances, arrange for an individual responsible for the space to provide access rather than issuing a key or credential.

(2) Temporary access

When access is only needed on a temporary basis and a key or credential is deemed necessary, a clear timeline and process for return should be determined and communicated at the time of issuance.

(3) Provide minimum level of access required

Issue keys or credentials that open the least number of spaces required for an individual to perform their assigned responsibilities.

(4) Card access

When possible, access should be issued via electronic access credentials rather than issuance of physical keys. Access provided through the electronic access control system is easier to control, monitor and audit.

(C) Roles and responsibilities

(1) Access control

University access control is charged with the following functions and responsibilities:

(a) Installing and managing all access control systems within Ohio university facilities.

(i) No department or tenant occupying any Ohio university facility may install, modify or operate any access control system within said facility without the express written permission of access control.

(ii) Requests for the installation of new access control devices or systems, or the modification of existing devices or systems, should be directed to the access control office.

(b) Ensuring that appropriate access control procedures are implemented and communicated to the campus community.

(c) Maintaining all access control systems, mechanical or electronic, in good working order.

(d) Controlling the production, issuance and transfer of keys and electronic access privileges.

(i) Outside duplication of University keys is strictly prohibited. Section 3345.13 of the Revised Code states: No person shall knowingly make or cause to be made any key for any building, laboratory, facility, or room of any university which is supported wholly or in part by the State of Ohio.

(e) Maintaining records related to the request, issuance, transfer, loss and disposition of keys and access credentials.

(2) Departmental responsibilities

It is the responsibility of each department head to designate an employee or employees to serve as the official departmental key contact(s) for their unit or area. Departments are responsible for the following functions:

(a) Departmental key contacts are the sole departmental authority as it relates to keys, cores, electronic access schedules, electronic access lists, and all other access control requests. Key contacts are responsible for requesting service from access control and ensuring appropriate dissemination of keys and access credentials.

(b) Departments and their designated key contacts are fully responsible for the proper tracking and issuance of keys and access control devices.

(c) Routine audits of key inventory and core disposition are recommended to enhance proper control and that key records are accurate and updated.

(d) It is the responsibility of each department to ensure that all keys or access credentials are retrieved from any employee, student, or contractor who is separated from the university due to any circumstances (resignation, termination, retirement, withdrawal, cessation of assignment, etc.) It is further the responsibility of each department to ensure that the access control office is contacted to revoke any electronic access privileges that a separated employee, guest, student, vendor, or contractor may have.

(e) Any lost keys or access credentials must be reported immediately to the access control office. Access control, in cooperation with other appropriate university departments, will conduct a risk assessment and recommend appropriate corrective action.

(i) Any cost incurred by the university as a result of a lost or compromised key or access credential will be billed to the university department responsible for the incident.

(f) Departments are responsible for notifying access control of any changes to building unlock schedules or access lists for facilities or areas equipped with electronic access control in a timely fashion.

(3) Key and access credential-holder responsibilities

Individual key / access credential holders are responsible for:

(a) Maintaining control, possession and security of all keys and credentials issued to them by Ohio university.

(b) Preventing unauthorized use or duplication of all keys and credentials to which they have access.

(c) Relinquishing and returning all keys and access credentials issued to them immediately at such time as they are no longer authorized or required.

(d) Immediately notifying their supervisor and departmental key contact of any lost keys or stolen credentials.

(D) Restrictions

(1) Emergency access provisions

For reasons of personal safety, all university access control systems must allow for master key operation by emergency services personnel (fire and police).

(a) Requests for spaces to be keyed off-master must be submitted to access control by the planning unit head in writing and include a detailed rationale and justification for the request.

(b) Such requests must be reviewed and approved by access control and the Ohio university police department.

(2) Issuance and control of master keys

Because master keys open entire areas or buildings and carry a significant level of risk if lost or compromised, access to them should be restricted to the fullest degree possible without impeding operations.

(a) In general, a building level or higher master key should never be taken off of Ohio university property.

(b) Departments or units should only maintain master keys in access controlled cabinets or key retainers within locked spaces whenever they are not in use.

(i) Access control recommends that master keys be maintained and stored in electronic key control cabinets to provide appropriate monitoring and tracking of their use. Contact access control for additional information.

(c) Requests for the issuance of master keys may require written approval of the planning unit head and should include a detailed rationale and justification for why a master key is required.

(d) Access control reserves the right to deny the issuance of master keys and propose alternative solutions that carry lower risk if sufficient justification of the need for a master key is not provided.

(e) Failure to report a lost or stolen master key may result in disciplinary action, up to and including termination of employment.

(3) Lockouts

In the normal course of operations (i.e., except in emergency situations), facilities management, access control, Ohio university police department (OUPD), and other service personnel are prohibited from providing access to locked spaces to individuals that are outside of their department. Individuals should contact their departmental key contact to arrange for another departmental staff member who has access to assist in the event of lockout situations.

(a) In the event of an extenuating circumstance after hours, OUPD may provide an individual access under the following circumstances at their discretion:

(i) The space is exclusively under the control of the individual.

(ii) OUPD is able to positively verify the individuals identity and their control of the space.

(iii) The need is a result of an extenuating circumstance (i.e., inadvertently locking keys inside of

the space).

(b) OUPD will not typically provide access under the following circumstances:

(i) The space is shared or communal locked spaces.

(ii) The space is residence hall space.

(iii) The individual has forgotten their keys.

Furthermore, the only department authorized to handle lockouts in residence hall spaces is housing and residence life. No other university personnel will provide access to occupied residence hall spaces under any circumstances.

(4) Building locking and unlocking

To provide for efficient and timely unlocking and locking of building perimeter doors, access control recommends the installation of electronic access controls to allow for automatically scheduled unlocking and locking of perimeter doors.

Facilities management only provides locking and unlocking of the perimeter doors on academic classroom buildings and other appropriate buildings where electronic access control is not available. Buildings that meet the above criteria will be unlocked sometime between five a.m. and seven a.m. and secured sometime between eleven p.m. and midnight on Monday through Friday only.

If a building requires a schedule that varies from the times listed, then unlocking and locking must either be handled by the department/unit or electronic access controls that allow for remote scheduling must be installed.

No unlocking service is available or provided for any interior doors at any time. It is the responsibility of the department that controls the space to enhance that anyone who has been authorized to use any space has access to that space as needed.

(5) Contractor and vendor access

Contractors and vendors who require regular or prolonged access to Ohio university facilities may be issued keys or access credentials at the request of a sponsoring department with the approval of access control.

Requests for contractor or vendor access should be directed to the access control office in writing at least forty-eight hours in advance. The request should include the following information:

(a) Name of the firm, vendor, or external entity

(b) Full name of all personnel requiring access

(c) Date and time range access will be required

(d) Buildings or spaces to which access is needed

(e) Reason that access is required

No keys or credentials will be issued to any outside entity without prior written notice and approval.

Contractor access to occupied residential space will only be granted when escorted by Ohio university personnel. No interior keys will be issued for occupied residence halls.

Any cost incurred by the university as a result of a lost or compromised key or access credential issued to an external entity will be billed to that entity.

(6) Internally and externally leased property

In the case when property is leased by the university from a third party, the lease may prevent conformity with this policy.

(a) The lease with a third party will dictate access control methods and procedures.

(b) When possible, the third party should allow access control to hold key(s) in the university key bank for emergency situations.

(c) The university department utilizing the leased property should designate a responsible key contact as described in paragraph (C) of this policy.

In the case when a university owned building or space is leased to an external party, this policy should be referenced in the lease.

(d) This policy is not applicable to ground leases where a third party developer constructs or owns the improvements.

(E) Appeals

Decisions made by access control as provided for in this policy may be appealed to the associate vice president for facilities management and safety.

The version of this rule that includes live linksto associated resources is online at

https://www.ohio.edu/policy/44-050.html