POLICY

Effective Date: September 1, 2015
Approved By: President Bruce Shepard

Authority: RCW 28B.35.120; SAAM Chapter 20
WAC 516-24-001

Cancels: POL-U5610.01 Issuing and Using University Keys

See Also:
- STN-U5710.01 Access Control Standards
- POL-U5346.01 Safeguarding & Safeguarding University Assets
- POL-U5950.01 Health, Safety and Environmental Protection
- POL-U1500.08 Using University Resources
- POL-U5315.25 Reporting Loss of University Funds or Property

POL-U5710.01 MANAGING ACCESS TO UNIVERSITY FACILITIES

This policy applies to all faculty, staff, students, volunteers, guests or visitors who access University owned and leased facilities and space. Its purpose is to facilitate access to space and equipment by authorized individuals, to safeguard members of the Western Washington University community, and to minimize risk to both the University's property and the personal property of the individuals who work, study, and reside at Western.

Definitions:

Access Control: The means, methods and practices used to minimize risk to persons and property by regulating entry to buildings and spaces. Control activities may be preventative and/or detective.

Access Device: Any University-authorized device used to lock/unlock mechanical and electronic door hardware, including traditional metal keys, ID card, application and/or any other electronic means of access.

Area Access Manager (AAM): An Executive Officer, Chair, or Director of an academic or non-academic department designated to grant access privileges to individuals (i.e. faculty, staff, students, vendors and volunteers) for space over which they have been granted authority.

Area Control Administrator: A position designated to have operational oversight for access control to a defined grouping of buildings, facilities or spaces, and is responsible for determining operating hours.

Authorized Individual: An individual (i.e. University faculty, staff, student, volunteer or contractor) for whom certain access privileges have been granted by an Area Access Manager.

Departmental Key Controllers: Positions designated by an Area Access Manager to perform access administrative duties in accordance with this policy (and related standards, procedures a d guidelines).

Sponsored Guest: A person who is present in the University building or space by way of an Authorized Individual

1. Vice President for Business and Financial Affairs Ensures an Appropriate and Effective Access Control Management Process is Established

The Vice President for Business and Financial Affairs (VP for BFA) will ensure physical access processes:

a) Are implemented and maintained,

b) Are compliant with other University policies, and

c) Minimize risk to the campus community and its property.

The VP for BFA appoints members of the Campus Access Control Committee (CACC) and approves its charter.

2. Campus Access Control Committee (CACC) Oversees Access Control

The CACC is a standing committee with the responsibility to:

a) Designate Access Control Administrators (ACA) for campus spaces,

b) Develop and maintain standards, procedures, and guidelines in response to policy objectives,

c) Advise vice presidents on access control issues within their divisions,

d) Advise ACAs in the development of processes for requesting and granting access devices within their areas of responsibility; and

e) Interpret this policy to resolve individual disputes and address questions pertaining to access control.

3. Area Control Authorities Define the Process for Requesting and Granting Access Devices

ACAs designate Area Access Managers (AAM) for areas and spaces assigned by the CACC. The specific process for requesting, and the criteria used for granting access and access devices, is defined by the ACA in accordance with campus guiding documents and divisional guidance. The following underlying principles apply:

a) Employment status does not imply automatic authorization for access,

b) Access is granted at the lowest level of need, and

c) Granting access is to always favor safety and security of persons and property over the convenience of the requester.

AAMs may only grant access privileges within the parameters established by an ACA, and only for the areas assigned by the ACA.

4. Guiding Documents

Guiding documents are an extension of this policy. The CAAC, ACAs, AAMs, and Authorized Individuals are required to follow approved guidelines in order to effectively manage access to University facilities. Guiding documents will include, but are not limited to:

a) Standards, procedures and guidelines for Issuing Access Devices - Describes levels of access and criteria for granting access privileges and access devices to authorized individuals.

b) Identification of ACAs and AAMs and departmental responsibilities for access control.

c) Access Control Measures - Describes risk and vulnerability considerations when determining the preventive and detective measures that will be used by the University for access to areas on campus.

5. Access to All University Owned and Leased Facilities and Space Limited to Authorized Individuals

a) During scheduled hours, academic and administrative buildings and spaces are open for general use by employees, students, and the public for educational, work related, and special event purposes.

b) Outside scheduled hours, access is restricted to authorized individuals. Sponsored guests must be accompanied at all times by an authorized individual.

c) During all hours:

i. Access to certain University areas is limited to authorized individuals only. For example:

1) Operational facilities and spaces (e.g. steam plant and mechanical rooms).

2) Higher-risk facilities and spaces (e.g. laboratories, hazardous materials storage areas, and performance venues).

ii. Access to residential facilities is limited to authorized:

1) Students,

2) Guests of students,

3) Employees,

4) Visitors (e.g. pre-authorized conference attendees), and

5) Contractors.

6. Visitors, Students and Employees Must Comply with University Conduct Regulations

In addition to employees and students, guests, contractors and visitors on University property are expected to comply with all University policy and state and federal regulations related to:

a) Access to and use of University buildings and spaces, and

b) Appropriate conduct as described in WAC 516-24.

7. All Access Devices Are the Property of Western Washington University

a) Access devices and privileges are assigned to authorized individuals on a temporary basis only,

b) Authorized individuals must sign for the access device, indicating they understand and will comply with individual rules and responsibilities for access devices,

c) Supervisors of authorized individuals must ensure access devices are promptly returned or relinquished to the original issuer:

i. When no longer needed for any reason,

ii. Before departing the University or transferring to another department, or

iii. Upon request for any reason at any time by an Executive Officer, Access Control Administrator, Area Access Manager, Supervisor, or Director of Public Safety.

d) Failure to return access devices by an authorized individual may result in one or more of the following:

   i. Administrative action by the University, up to and including legal action, and/or,

   ii. Assessment of charges for expenses incurred by the University to return access control to the same level that it was before it was compromised by the individual's failure to return the access device.

e) Lost, stolen, or damaged access devices shall be reported immediately to the:

   i. Appropriate Access Control Administrator,

   ii. Area Access Manager, and

   iii. University Police Department.

The Reporting Loss of University Funds or Property (POL-U5315.25) policy is to be followed when any known or suspected loss resulting in the unauthorized taking of University (public or non-public funds or property or other illegal activity.

7. Authorized Individuals Responsible for Safekeeping Access Devices and Appropriate Use of Spaces

Authorized individuals who are assigned an access device are prohibited from:

a) Loaning access devices to others,

b) Transferring access devices to others,

c) Duplicating access devices,

d) Altering access devices or access control mechanisms,

e) Damaging, tampering, or vandalizing any university access control mechanism,

f) Propping locked doors open, and

g) Admitting unauthorized individual(s) into an access controlled space.

9. The Director of Public Safety Ensures Audits of Issued Access Control Devices

The Director of Public Safety may independently conduct periodic audits of issued access control devices or may request that Area Control Administrators and Area Access Managers conduct audits of the area(s) for which they have oversight.