STANDARD

Effective Date: February 16, 2017
Approved By: Campus Access Control Committee Authority: POL-U5710.01

CAMPUS ACCESS CONTROL STANDARDS & PROCEDURES

General:

The safety and security of our Institution, its physical space and assets is a shared responsibility of all members of the University community. To meet this obligation, the University has established an Access Control policy. These supporting standards and procedures, which are an extension of the policy requirements, address the issuance and accountability of all keys and electronic credentials which control access to University buildings and their contents. Access Management may be delegated onto University departments that are able to perform that function in compliance with University policies and standards. Access Control privileges are determined and assigned by University administrators based on the specific needs and requirements of the University and the individual key/electronic credentials holder.

These standards are established to provide deans, directors, and department chairs information and authority to audit and regulate the issuance, transfer and return of all keys and building access credentials. These standards also outline the responsibilities of academic and administrative leadership, as well as the holders (Authorized Individuals) of keys and electronic access credentials.

Individuals may be granted access to spaces for which they have a regular and recurring need for entry due to official university business. All decisions to authorize access as well as the level of access authorized will take into consideration the security and safety needs of the entire University community. It should be emphasized that community safety and security, and university needs will always take precedence over personal convenience.

It is the policy of the University that other than during normal working hours, all buildings shall be locked in order to maintain the safety and security of both the buildings and the contents. Keys are issued for entry to University buildings for the purpose of conducting University business only.

Authorized Locks, Keys, and Electronic Access Credentials

All installations, modifications, or changes to access control systems and equipment shall be performed by or overseen by Facilities Management under an approved work order or Facilities Development and Capital Budget under a building project contract.

Every building, office, classroom and other University owned spaces will be keyed to Western's grand master system. Each building will be keyed to a specific building master key, which may be used by approved academic, administrative, or facilities management personnel. In addition, there may be several levels of mechanical or electronic access devices that permit limited access by selected individuals or groups to one or more offices or spaces within a building. No campus building, office or other space will be secured by any locking device that is inconsistent or incompatible with the campus keying standard.

Commercially leased spaces are not covered by these standards. Modular workstations with doorways are not covered by these standards.

Definitions

A. **Check Out Keys** – Keys or electronic credentials temporarily issued to students or staff for after-hours access to labs, classrooms, and other academic spaces.

B. **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.

C. **Access Credential** – 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.

D. **Access 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.

E. **Area Access Manager** – A Manager, Supervisor, 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.

F. **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.

G. **Building Access** – the capability of entering a building during hours of the day when the building is closed. Access is achieved by using a brass key or electronic access credential.

H. **Building Master Key**- a master key which operates all or most locks in a given building

I. **Building Entrance Key**- A key which operates the lock on one or more outside entrance doors to a building.

J. **Desk/Cabinet Access** – The capability of locking or unlocking a specific desk, cabinet, or other furniture item. Access is achieved by a key that is handed from individual to individual on a case-by-case basis. No key tracking exists at the University level.

K. **Department or Area master key -** a master key which operates all or most locks of a given department. The number of locks on a given departmental master will be limited to reduce overall risk.

L. **Departmental Key Controllers** – Positions designated by an Area Access Manager to perform access administrative duties in accordance with University policies and procedures.

M. **Grand Master Key**- A key which operates multiple locks on doors of multiple buildings on the main campus.

N. **Room Access** – the capability of entering a specific room or group of rooms within a building.

O. **Room Key** - A key which operates the lock on the door to a single room or a set of functionally grouped rooms.

P. **Sealed Work Rings & Keys.** Rings of multiple keys where the keys cannot be removed from the ring without cutting the ring. They are primarily assigned to trades, maintenance, technicians and custodial employees, and contractors and vendors during working hours and returned to a designated secure location at the end of a work shift.

Q. **Selective (or Area) Master Key** – A key that operates functionally similar spaces in multiple buildings.

R. **Sponsored Guest** – A person who is present in a University building or space by way of an Authorized Individual.

S. **Take Home Key** – A key or electronic credential issued to an authorized user which is intended or permitted to be taken off campus at any time.

Basic Standards for Key & Electronic Access Credential Accountability

Keys and credentials may be issued to faculty, staff, currently enrolled students, contractors or other essential personnel based identified need for access and consistent with job responsibilities or class/research requirements.

Keys and WWU issued credentials remain the property of WWU. No keys may be duplicated or loaned or transferred to any other person by the key holder. Facilities Management is the only authorized supplier for University keys.

Lost or Stolen Keys

In the event a key is lost or stolen, the Access Control Administrator who is responsible for the affected area will consult with the Director of Public Safety to assess the risk and determine whether rekeying needs to occur. While it is expected that any rekeying costs will be a divisional responsibility, units, programs, and departments may incur costs according to divisional protocols and administrative practices. Depending on the key type and its scope of access, this re-keying expense can be extraordinary. It is not limited just to the expense of replacing the one lost or stolen key. It may include the cost of re-coring and re-keying a whole building or multiple buildings.

Fees for keys not returned are the responsibility of the approving department. If the approving department wishes to recover any of these costs from an employee, they must work directly with Human Resources to accomplish that cost recovery.

Accountability

Keys and electronic access credentials are considered university assets. Academic and administrative leadership are responsible for safeguarding any keys and access credentials issued to, held by, or used in their departments, to include establishing appropriate safeguards and protocols consistent with these procedures that are necessary to secure, protect, preserve, and regularly account for those credentials.

Storage of Non-Take Home Keys & Access Credentials

Not all work keys approved for use by an Authorized Individual will be held by that person all the time. Depending on a key's scope of access, some keys may be held by a person and some keys will only be available as needed during the workday from a locked key control cabinet on campus premises. When not in use, those keys must be stored in a locked key control cabinet approved by Facilities Management. Grand Master and Building Master keys will generally not be issued unless required for uniquely determined job responsibilities. When issuance is authorized, All Grand Master and Building Master keys are issued for one-day, secure check-out only and may not be taken off of the campus. All Grand Master and Building Master keys shall have an attached, approved tracking device and shall be stored in a cabinet approved by Facilities Management.

Audits

Access authorization may be delegated to University departments that are able to perform that function in compliance with University policies and standards. Compliance is determined by way of an annual self-audit by departments.

The annual audit will be initiated by Facilities Management and will include the following:

- A list of all keys and access credentials issued to each department/area will be sent to each Area Administrator for the purpose of verifying the physical presence of the keys and credentials.

- A list of all individuals who the respective Area Access Manager has approved for access into their designated spaces for the purpose of confirming these individuals continue to need access.

Sensitive Areas

Access will be restricted or controlled for certain areas with specific safety and security concerns. These areas shall also be considered for additional security measures in order to mitigate environmental conditions.

Level	Life Safety or Information Concern	Security Measures for Consideration
Level A	General Access; non-sensitive information	N/A
Level B	High dollar value item(s) in space – single value or cumulative value Privileged information External doors to Buildings and University Residences	Key or card access UPD monitoring recommended
Level C	Life threatening, dangerous or controlled material stored or used in space; Sensitive (FERPA, HIPAA, Law Enforcement, etc.) information in space; Sensitive research Server Rooms	Limited individual access authorized Controlled access through electronic card entry recommended UPD monitoring requirements to be determined with input from Environmental Health & Safety

Roles & Responsibilities

The following personnel are designated **Access Control Administrators** (ACA). These ACAs have operational oversight for access control to a defined group of buildings, facilities, or spaces.

FACILITY/SPACE TYPE	ACCESS CONTROL ADMINISTRATOR
Academic and Administrative Buildings Including, but not limited to offices, classrooms, general use classrooms, laboratories, administrative spaces, storage rooms and mercantile spaces within academic & administrative buildings	Director of Space Administration and Management
Housing and Dining Facilities	Director of University Residences
Facilities Operated by the Viking Union	Viking Union Facilities Director
Wade King Student Recreation Center	The Director of Campus Recreation
Building Operations and Infrastructure Spaces: Physical Plant spaces, all mechanical rooms, electrical rooms, custodial closets, roof access, tunnels, etc.	Director Facilities Management
Infrastructure Spaces Pertaining to Information Technology and Telecommunications	Chief Information Officer (CIO)

<u>Access Control Administrators (ACA) Responsibilities</u>:

1. Appoint Area Access Managers and provide Facilities Management with a list of buildings and/or rooms numbers under each Area Access Manager’s delegated authority.
2. Require from their designated Area Access Managers a record-keeping system that will ensure accountability and security for all Area Managed keys.
3. Determine operating hours of their spaces.
4. Define the process for requesting access to their spaces and the criteria used for granting access to such spaces.
5. Approve the designation of departmental key controllers by Area Access Managers.
6. Approve issuance of Building Masters and Area Masters within their areas of responsibility.
7. Obtain concurrence from the Director of Public Safety and all affected Access Control Administrators when proposing to issue area master level and above keys.
8. Consult with the Director of Public Safety to assess the risk and determine whether rekeying needs to occur.
9. Review and approve/disapprove annual key and card access audits
10. Initiate key control or electronic access control reports as needed.

Director of Public Safety Responsibilities:

1. Designated as the overall Campus Security Officer & Co-Chair of Campus Access Control Committee.
2. Approves issuance of Building Master and above keys upon recommendation of Access Control Administrator(s).
3. Directs responsible employees to conduct a key control record audit as needed,
4. Directs responsible employees to conduct an electronic access control system audit as needed,
5. Directs designated responsible employees to conduct surveys and audits of campus departments and units to determine the level of adherence and implementation of the access control-policy;
6. Reports the results of key control and electronic access control record audits of campus departments to the Vice President over the area being audited and to the Vice President of Business and Financial Services, at regular intervals.
7. Determines if rekeying is to occur in the event that a key is lost or stolen. Decisions to rekey or to duplicate keys are based on consultation with Risk Management and the Access Control Administrator(s).

Facilities Management:

1. Responsible for creating and maintaining the University's lock and key system, including schematics, codes, product standards, and service equipment.
2. Responsible for maintaining and operating the University's electronic access control system.
3. Conduct annual audits of issued keys and authorizations approved by campus access authorities, and report results to the Director of Public Safety.
4. Maintain a computer database of all keys/credentials, key holders, locks, and associated building and room numbers that they operate.
5. Help departments set up a key record and security system when requested.
6. Provide education and training on access control.
7. Develop keying schedules, re-key and stock necessary locks, cylinders, key blanks, and related hardware.
8. Supply contractors with WWU cylinders for new and renovated buildings through appropriately funded work order.
9. Ensure access requests have obtained appropriate Area Access Manager approval for access into the assigned space
10. Maintain the key control filing system and records regarding all key systems.
11. Produce key control or electronic access control reports to campus authorities as requested.
12. Fabricate or procure all keys.
13. Issue all keys/credentials to individuals and Department Key Controllers.
14. Enable electronic access to Authorized Individuals.
15. Remove electronic access from staff & students who no longer need access
16. Deactivate lost or stolen electronic credentials
17. Conduct all maintenance and repair work regarding mechanical locking systems.

18. Consult with the Director of Public Safety (or designee) concerning records of keys lost or stolen.
19. Facilities Management is accountable for maintenance of up-to-date and accurate key control records.

Area Access Managers (AAM) are Managers, Supervisors, Chair, or Directors 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. The AAM is responsible to:

1. Appoint departmental key controllers, and advise Facilities Management and the Lock Shop, in writing, of the appointment (See Form).
2. Establish and implement a record-keeping system that will ensure accountability for all Area Managed keys.
3. Complete annual key and card access audits.
4. Complete a key audit upon the change or departure of a Departmental Key Controller.
5. Maintain appropriate departmental records subject to an internal audit
6. Protect keys from loss, theft, or unauthorized use through storage and accountability of check out keys in an approved tamper resistant lock box.

Departmental Key Controllers are positions designated by the AAM to perform access administrative duties in accordance with these standards.

1. Complete a Key Request form or Access Card Request form to assist employees with the request for a new, transfer or replacement key for doors within the Area Access Manager's delegated authority.
2. Act as the administrative proxy with the Lock Shop by picking up keys for departmental employees, issuing those keys to those employees or students, and notifying Facilities Management of such action.
3. Issue check out keys to students and departmental staff. This includes keeping accurate administrative records of who individual keys have been issued to and collection of those keys once an individual has left or no longer requires access.
4. Document the issue and return of each key on a "Key issuance and acceptance form". Provide copies of the signed form to Facilities Management.
5. Retains all keys not issued to a specific individual in an approved, tamper resistant lock box. (Facilities Management will provide specifications for approved lock boxes.)
6. Notify Facilities Management when an individual has left, no longer requires access, has returned a key, or when a key has been reissued to another individual. (Keys are issued to individuals and will remain in the key holder's name until the Lock Shop receives and processes notification of a key return or transfer.)
7. Complete an annual audit for all individuals who have key or electronic credential access to your department/area
8. Report lost or stolen keys and/or access cards immediately (within 24 hours of discovery) to the University Police, Access Control Administrator, and the Area Access Manager.

9. The delegation of duties by the AAM to a Departmental Key Controller does not relieve the AAM of his or her ultimate responsibilities as set forth in these standards.

Key or Electronic Credential Holders – University Personnel and Students

1. The holder of a key/credential to any University facility or space assumes responsibility for the safekeeping of the key and its use. When leaving a campus space or building, the holder is responsible for ensuring all doors, windows and other physical points of entry into the building are at a minimum as secured as they were upon arrival. If it is not possible to secure this space, he or she is responsible to notify UPD Dispatch of the situation.
2. Never loan a key or credential to someone not registered as the key or credential holder
3. Report lost or stolen keys or credentials to supervisor and Departmental Key Controller immediately.
4. Return keys and/credentials to the department Key Controller or Facilities Management immediately at end of employment term or change in employment terms or location (e.g., transfer to a different unit, change of responsibilities)
5. Return all departmental work rings and keys to the designated secure location prior to departing the work place.
6. Prevent other individuals from entering space for which they are not approved (i.e., tailgating in behind someone passing through a locked entry)

Key or Card Holders – Contractors, Consultants, Vendors, and other Non-University Personnel

1. Non-University personnel are not permitted to remove University keys and access credentials from University property. All keys and access credentials must be checked out and checked in daily at the University Police Dispatch office.
2. Before keys may be issued, the Contractor shall present a signed letter on company letterhead indicating the names and positions of employees authorized to check out keys on behalf of that company, and that the company is assuming financial responsibility for all re-keying required to restore security due to keys lost or not returned. The University's project or contract manager will be responsible for issuance and return of keys.
3. The holder of a key to any University facility or space assumes responsibility for the safekeeping of the key and its use. When leaving a campus space or building, ensure all doors are as secured as they were upon arrival.
4. Report lost or stolen keys to the project or contract manager and University Police Department immediately upon discovery.
5. All keys must be returned to the Facilities Management upon completion of the project.
6. Prevent other individuals from entering space for which they are not approved (i.e., tailgating in behind someone passing through a locked entry)

Requesting Access

Requests for access shall be routed through the appropriate chain of command, with the Supervisor of the Requestor confirming the regular and recurring need for access. In general, requests should identify the spaces which the individual needs access to. Facilities Management make the determination as to which key(s) or credential(s) best accommodate the request. In some cases, the best accommodation may be to request the assistance of University Police personnel.

- Keys or credentials for spaces within the authority of an Area Access Manager may be acquired via online request form submitted by a supervisor, through the Area Access Manager, to Facilities Management.
- Keys or cards for other work locations must be approved by the designated Area Access Manager in which the space is located
- Access is granted through issuance of a key or through the individual's electronic access credential. Issuance of keys is to individuals by Facilities Management. or Departmental Key Controller.
- Area Access Managers and Departmental Key Controllers may be authorized to issue departmental check out keys when those managers have established reasonable accounting and reporting procedures. These procedures will be approved by the Access Control Administrator(s).
- When access requests are approved, access parameters for individual key or card holders are designated according to these guidelines and individual access parameters are registered with Facilities Management.

2016 Campus Key Authorities & Eligibility

Key Type	Eligibility to Carry	Approval Authority	Issuing Entity/Conditions
Great Grand Master	N/A	N/A	Will not be issued
Grand Master	University Police Officers	Vice Presidents	With the safety & security risk posed by the potential loss of a grand master, special conditions apply to the accountability and storage of these keys: • Work rings, checkout basis only. • Grand masters shall not be removed from campus. • When grand masters are not in use, these must be stored in an approved lock box. • All grand master key issuances shall require use of a tracking device or tether when removed from the authorized lock box. Issued by: Facilities Management.

Building Master	Emergency response personnel. President, Vice Presidents, Access Control Administrator, designated permanent faculty & staff Designated service personnel (Facilities Management, Facilities Development, Academic Computing, Telecomm, Transport Services, Space Management, University Residences)	Director of Public Safety Dean or Vice President Access Control Administrator(s)* *Work rings may be issued to service personnel according to divisional protocols.	With the safety & security risk posed by the potential loss of a building master, special conditions apply to the accountability and storage of these keys: • Work rings, checkout basis only. • Building masters shall not be removed from campus. • When building masters are not in use, these must be stored in an approved lock box. • All building master key issuances shall require use of a tracking device or tether when removed from the authorized lock box. Issued by Facilities Management
Selective Master (or Area Master)	Emergency response personnel. Designated service personnel (work rings, check out basis only, as needed to perform their duties)	Director of Public Safety Access Control Administrator(s) Area Access Managers	• Work rings, checkout basis only. Issued by Facilities Management directly or through Departmental Key Controller
Department or Area Master (Sub-Master)	Employees under the AAM jurisdiction,	Area Access Manager	Issued by Facilities Management directly or through Departmental Key Controller
Building Entrance & Room Keys	Faculty, staff, or student employees	Area Access Manager	Issued by Facilities Management directly or through or Departmental Key Controller

Building Entrance & Room Keys	Contractors & Vendors	Dependent on Level required	Issued by Facilities Management

Returning Access Devices

Return all access devices to the issuing entity (Facilities Management or Department Key Controller) when access is no longer required, before discontinuing employment, or upon transferring from a current position. Do not turn devices over to the person assuming your position.

Annual Inventory

Annually, Facilities Management will develop and send to each college, department, individual, or Area Access Manager a list of access devices they have been issued. Once the responsible college, department, individual, or Area Access Manager receives the list from Facilities Management it shall complete and return the results of the audit to Facilities Management no later than February 1. New or replacement keys will not be issued to a department which has not completed the annual audit.

1. Checkout Key Accounts
   Each AAM shall complete an inventory of their area and certify that all devices are secured and/or accounted for (i.e. issued to a current Authorized Individual).
2. Grand Master & Building Master Keys.
   Each entity receiving such a list shall complete an inventory and certify that all devices are secured and accounted for.
3. Service Provider Work Rings (Facilities Management, Telecomm, Transport Services, EHS, etc.)
   Each entity receiving such a list shall complete an inventory and certify that all devices are secured and accounted for, and are stored in a secure location when not being used by on-duty personnel.
4. Contractor Access.
   Project or contract managers will receive a list of contractors and personnel they have authorized to receive access devices, and certify that all devices are accounted for.