Access Control Standard and Protocols

July 2017

PURPOSE:

The purpose of this standard is to establish guidelines on the issuance of access devices to authorized users (employees, students and affiliates) in order to gain entry to certain facilities.

This standard is necessary in order to describe specific responsibilities, conditions and practices designed to address critical access needs in a manner that minimizes risks and maximizes the protection of individuals, physical assets and private information within the control and/or ownership of West Virginia University ("University").

Standards and Protocols:

The safety and security of the University's community, physical space and assets is a shared responsibility of all members of the University community. It is the practice of the University that access to the University's facilities is controlled in order to prevent and/or limit potential loss.

To meet this obligation, the provisions set forth below address the design, administration and management of access control systems and measures to ensure their integrity.

Access to the University's facilities is considered a privilege, and is determined and assigned based on the specific needs and requirements of the University and the user.

DEFINITIONS:

Access shall mean the ability to gain entry into an area, space, and/or facility by means of access device.

Access Devices shall mean all devices and items provided to an authorized user for purposes of providing access. Such access devices may consist of traditional metal key(s), Mountaineer Cards, proximity devices and temporary ID cards, or any electronic means of access (e.g., CBORD and ONITY).

Building Master Keys shall mean any combination of electronic card access and traditional metal keys that have access to open multiple doors on the campus. Due to security concerns and the significant cost associated with the loss of a Building Master Key, such keys will only be provided to the individuals listed below upon request after verification from the University's Police Department:

(1) Deans of Schools
(2) Chief Administrators (for control of specific areas of responsibility)
(3) Facilities Management Personnel
(4) Others may be approved in consultation with UPD.

CBORD shall mean the electronic access technology that allows authorized users to use a Mountaineer Card as the means of gaining access. CBORD replaces traditional keys with an electronic card reader that is networked into the current Information technology infrastructure to allow for remote communication. The electronic access readers can be horizontally or vertically swiped. Current standards indicate that CBORD locks are to be used on perimeter doors and in interior spaces where applicable due to high turnover volume, security concerns, main entry to suites and possibly other conditions.

Other Electronic Devices shall mean the electronic locks used to secure interior rooms and facilities, such as mechanical rooms, offices, and other interior spaces that do not have direct access to the building's exterior. The specific systems are very much like a hotel access lock, they are a stand-alone device, offline lock, and unlike CBORD, they only have the capabilities of being programmed locally at the lock with a hand held programmer, and cannot provide remote lockdown. This style of offline electronic lock stores all access history and is maintained in the lock's memory that requires periodic visits to download/upload information and for battery replacement. This type of device is not designed, nor permitted for installation at doors leading to a building's exterior.

Department Master Keys shall mean any combination of electronic card access and traditional metal keys that have access to multiple doors within a specific office suite or department space on the campus. Due to security concerns and the significant cost associated with the loss of a Department Master Key, such keys are only distributed to individuals specified by the Department Head, or a Chief Administrator, and must be approved by the assigned department building supervisor.

Great Grand Master Key shall mean any combination of electronic card access and traditional metal keys that have access to open **ALL** doors and entry points on the campus. Due to security concerns and the significant cost associated with the loss of a Great Grand Master key, such keys shall only be provided to the individuals listed below upon request after verification from University's Police Department:
(UPD and Facilities Recommends NOT Issuing a Great Grand Master to Anyone)

(1) President of the University
(2) Provost of the University
(3) Vice President
(4) Associate Vice President, Facilities and Services
(5) Chief of Police and delegates
(6) Facilities Management Personnel
(7) Access control technicians (i.e., Locksmiths)

Suite Master Keys shall mean any combination of electronic card access and traditional metal keys that have access to multiple doors within a specific office suite or department space on the campus. Due to security concerns and the significant cost associated with the loss of an Suite Master Key, such keys are only distributed to individuals specified by a Dean of a College or School, a Chief Administrator, or Facilities Management, and must be approved by the assigned department building supervisor.

Sub Master Keys shall mean any combination of electronic card access and traditional metal keys that have access to multiple doors on a floor on the campus. Due to security concerns and the significant cost associated with the loss of an Sub Master Key, such keys are only distributed to individuals specified by a Dean of a College or School, a Chief Administrator, or Facilities Management and must be approved by the assigned department building supervisor.

Residence Keys shall mean any combination of electronic card access and traditional metal keys that have access to doors within a student's assigned living area on the campus. Students are only issued access for the building in which they reside and Mountaineer Cards will register invalid when used in another residential building. Residence Keys are only distributed to the Residential Life Office for issuance to a student, and must be approved by the assigned department liaison.

Employee shall mean all full-time and part-time faculty and staff members, temporary/casual workers, as well as workers employed on a per diem basis, and student employees.

Student shall mean all person registered for one or more classes at WVU, including on-line classes.

Affiliates shall mean non-employee members and non-students of the university community that include but are not limited to: vendors, volunteers, observers, trustees, members of the citizens' board, dependents of employees, retirees, emeriti faculty, alumni, summer scholars, summer campers, Wellness center members, tenants (non-WVU staff) renting space in a University owned buildings and our private partnerships.

KEY Control Manager- The individual appointed by the senior building administrator to manage the building access system, usually this is the building supervisor.

Power users shall mean those Building Supervisors and/or Building Administrators who have the ability to provide access to their respective building(s). The designation of power users is based upon the volume of programming changes and building use.

Security Levels Defined:

Level 1 - "Basic Security": These areas are typically unlocked during business hours, allowing access by University personnel or the general public. After hours these areas are secured and access is by key or card access. University support units, such as custodians may have access to these areas.

Level 2 - "Enhanced Security": Areas that are mechanically and electronically locked at all times, including during normal business hours, require key or card access to gain entry each time. University support units may have access to these areas. Security Systems are also integrated into this program and may be required to be armed and disarmed by authorized personnel, as necessary, to maintain the desire level of security.

Level 3 - "High-Risk Security": Areas that based on grant, research, and risk as determined by UPD or by federal, state, or local laws or code have restricted access, or are restricted by University policies and/or procedures. These areas may require higher security access control devices such as biometric control devices. In some cases access by University support services may be restricted or limited and may require that support services be escorted by approved department personnel. Security Systems are also integrated into this program and may be required to be armed and disarmed by authorized personnel, as necessary, to maintain the desire level of security.

Procedure for Mechanical Keys:

A. REQUESTS GENERALLY – Basic Security and Enhanced Security

All requests for access must be made by designated Building Supervisors to Facilities Management. Once a request is received via a work order, Facilities Management will process the request, based upon the type of access requested. A person requesting access must meet the applicable criteria as outlined in this section. All areas requesting “high risk security” must have area supervisor and UPD review and approval

Generally, all routine work, such as the initial installation of access devices, maintenance and repair of access devices will not be considered a billable request. However, in cases where an employee requires access to be reissued due to the loss or theft of an access device, the costs associated with the new access device will be billed to the requesting department. All non-billable/billable items are subject to review and final determination will be made by the Access Control Lead and/or Manager.

B. TYPES OF ACCESS AND CORRESPONDING APPROVAL

Faculty/staff, students and affiliates may require different types of access. There will be four (4) types of access requests. Each type of request has corresponding approval process, determined by the level of risk and exposure to the University in granting the access. It is the responsibility of all users to abide by this standard and to adhere to the levels of approval outlined below when providing access to an employee, temporary employee or casual worker.

1. LEVEL 1 ACCESS – Security Level 1
Requests at this level seek access to a single door. Such a request is considered the most basic type of access request, and only requires approval from building supervisor.

2. LEVEL 2 ACCESS – Security Level 1
Requests at this level seek access to multiple interior doors with a department, and access to doors leading to the exterior of the building during normal business hours (7:00 am to 7:00 pm, Monday through Friday.

3. LEVEL 3 ACCESS – Security Level 1
Requests at this level seek access to: (I) access to multiple buildings. Such a request must be reviewed and approved by <u>all</u> building supervisors impacted before submission to Facilities Management.

4. LEVEL 4 ACCESS – Security Level 2 and 3
Requests at this level seek access to restricted or high security areas. Such a request must be reviewed and approved by the building administrator or the Chief of Police before a work order is issued by FACILITIES MANAGEMENT.

<u>NOTE:</u>

Electronic Override Access Building Supervisors shall have an electronic override key to allow emergency access when electronic locks fail.

SEPARATION FROM THE UNIVERSITY; INTER-DEPARTMENT TRANSFERS; LEAVES OF ABSENCE

A. EMPLOYEES

1. SEPARATION

Where an employee is separated from the University, it is the responsibility of the immediate supervisor or Human Resources representative to collect all University owned materials including (metal keys, Mountaineer Card, proximity devices, and

temporary cards) previously issued to an employee. The department liaison will be expected to: (i) consult with the Key Shop/Access Control Shop to ensure that all devices are accounted for prior to separation; (ii) initiate a work order for the Access Control Shop to terminate all access in the system for electronic devices and (iii) submit all collected access devices to Key Shop or Access Control within 24 hours of collection, to enable proper and timely deactivation.

2. TRANSFER

If an employee is transferring to a new department within the campus, the current department liaison must submit a request to deactivate the employee's access. The employee's current liaison is responsible for collecting any keys issued to the employee prior to the effective date of the employee's to another department. Those keys are to be returned to the Lock Shop to properly document the return of the keys. The liaison in the new department shall be responsible for requesting access for the transferring employee in the manner described in Section I above.

3. LEAVE OF ABSENCE

Employees who are on a continuous leave of absence or on work-at-home assignment may be required to submit their access devices to their department liaison prior to the commencement of their leave/assignment.

III. VIOLATIONS of Standards

Violations of this standard may result in the loss of privileges afforded. Employees determined to have violated this standard may be subject to disciplinary action up to and including termination of employment. Violations include, but are not limited to, the following:

- loaning an access device to another individual;
- obtaining and issuing an access device without authorization;
- unauthorized duplication of access devices;
- damaging, tampering, vandalizing, altering or modifying University access devices, hardware; locks or other access mechanisms;
- installing or causing to be installed an unauthorized locking mechanism on University spaces (e.g., offices, labs, etc.);
- Propping doors open to avoid the use of access devices;
- admitting unauthorized person(s) into the building;
- failing to return an access device when requested by the Access Control Shop, UPD, the issuing department, or upon leaving the employment of the University;
- failing to report missing access devices;
- failing to comply with the request and approval provisions set forth in this policy.

 key boxes are not typically allowed to be kept within offices and/or departments with University keys. When key boxes are utilized primary records will reflect location and to whom the keys are issued, purpose, and date returned and access must be limited.

Manufacture of Keys

The Key/Lock Shop will make all keys once a completed form has been received. The key will be issued in the name of the department with the Key Control Manager listed as the custodian for the key.

Primary Records

The Key/Lock Shop will maintain the primary records for all keys issued. Records, at a minimum, will include the following information for each key issued:

- Key Number
- Building(s)
- Room(s)
- Department
- Building Supervisor
- Date
- Signature of Building Supervisor receiving key

On an annual basis, the Key/Lock Shop will prepare a list of those keys issued to all departments on campus. This list will be distributed to the Building Supervisor/Key Control Managers for verification of the records. Any corrections to the primary records will be made by the Key/Lock Shop based on the information provided by the Building Supervisor/Key Control Managers. While this must be done on an annual basis, an individual department can request a list of all keys issued in its name at any time.

Secondary Records

Each Building Supervisor will have the responsibility for those keys that have been issued to a particular building. This responsibility includes proper maintenance of the Key Assignment Forms, which are provided with each key. These forms will allow keys issued to a particular building to be transferred among individuals in that building without involvement of the Key/Lock Shop and will include the following information:

- Department
- Key Number
- Building(s)
- Room(s)

- Issue Date
- Issued to
- Issue date
- Received by building supervisor
- Return date
- Returned by building supervisor

These records or their computerized adaptation will be subject to review by the Internal Audit Department during both routine and surprise audits of departmental procedures.

Return of Campus Keys

Building Supervisors are responsible for collecting keys from individuals upon their departure from the University. Excess keys should be monitored and returned to the Key/Lock Shop when no longer needed. Excess and unnecessary keys in circulation create a security risk to the individual departments.

Lost Keys/Access Devices

In the event that a key is lost, the building supervisor should report the loss immediately to the Key/Lock Shop. The building supervisor must make individuals in his/her building aware that lost keys should be reported immediately. To obtain a replacement key, a new Key Request/Record Form must be completed. There may be a charge for lost keys.

Worn, Damaged, or Broken Key Replacement

A replacement for a worn or broken key will be provided by exchange for the defective key. The building supervisor should simply notify the Key/Lock Shop of the problem and turn in the defective key when picking up the replacement. Normally, at no charge.

Key/Access Device Duplication

It is strictly prohibited to attempt to have any University key duplicated by anyone other than the University lock shop.

Building Use Keys/Access Devices

Groups of keys may be provided to a building supervisor for local issue to students and other temporary uses provided the building supervisor supplies Facilities Management Department with evidence of an acceptable key record/retrieval system in the form of a

written procedure. Keys are to be requested using the standard Key Request/Record Form or a work order. The name on the request should be the administrative department and the card must be signed and approved by the appropriate building supervisor or higher.

The building supervisor is responsible for individual record keeping of the issued keys. Their records plus keys on hand should always match the record of the number of keys issued by Facilities Management Department.

Procedures for Mountaineer Card Access System

Issuing Access Cards

All WVU Cards will be issued by the Information Technology Services, Human Resources, Health Science Center, and Regional Campuses.

Employees/Affiliates

Once the Cbord system has the employment information for an employee including departmental name a card of the correct design can be printed by a card production office.

Students

Once the CBord system has current registration information, current housing information, or next semester registration information a Student card can be printed by a card production office.

Conference

Participants' request for special cards for guests visiting the University as participants in conference programs will be coordinated through the Information Technology Services.

Building Access

Employees

All requests for access for an employee require that the employee have an employee WVU ID number and a Mountaineer Card. Once an employee receives their identification number and Mountaineer Card through Human Resources, the employee’s departmental liaison must submit a request to the building supervisor to activate interior/exterior access.

Facilities Management Personnel

All access request for electronic entry for Facilities Management Personnel shall be requested by the employee's Manager via work order to the WVU Lock Shop.

Students

The University's Office of Enrollment Management is responsible for entering the new student's information into the University's system. The CSGOLD system downloads new information from the University's registration system every night. Once downloading is completed, a new student's card is updated with access to their residence hall building, libraries, pool, and other common areas on the campus.

The University's Office of Housing and Residential Life is responsible for providing access to residential students for their particular living areas. Residential students will only be granted access to their assigned living spaces and their Mountaineer Cards will register invalid if a student attempts to enter a different residential building.

Lost/Stolen Cards

Reporting lost/stolen cards is the responsibility of the card holder. A card holder may not permit any other person to use the card assigned to the card holder. Replacement cards will be issued by the Information Technology Services. There will be a charge for replacement cards.

Worn/Broken Cards

A replacement for a worn or broken card will be provided by exchange for the defective card. Replacement cards will be issued by the Information Technology Services. There will be a charge for replacement cards.

Primary Records

Information Technology Services will maintain the primary records for all cards issued. Records, at a minimum, will include the following information for each card issued:

- WVU ID Number
- Name Printed on Card
- Type of Card Printed
- Date Card was printed

On an annual basis, the Building Supervisor will be responsible for reviewing all faculty, staff, and non-WVU employees on campus who have access to their building. Verification will be to determine the accuracy of the automated records on file.

Online Lock owners\Building Supervisors receive a list of employees with a termination date in the past that are in a patron group that is managed by them for ex-employees who still have access to their locks each week.

Building supervisors/key managers shall in turn keep records of desk cards issued by them to include card #, issued to, date, date returned or deactivated, and signature.

All records of audits by building supervisors/key managers are to be maintained for three years. Spot audit may be performed by IT, Facilities Management, or the UPD and they shall also keep their audit findings for three years.

Secondary Records

Each building supervisor will have the responsibility for maintaining records of those building access cards that have been issued to their building. This responsibility includes proper maintenance of access request forms. These records will be subject to review by the Internal Audit Department during both routine and surprise audits of the departmental procedures.