Master Draft retrieved from CPSO - 3/21/17

Version Date of Draft - 7/11/11

3.100 UNIVERSITY PHYSICAL SECURITY & ACCESS CONTROL POLICY

3.101 Introduction and Purpose

A. The University is committed to the safety and security of all members of its community by maintaining the security of its facilities and physical environs. While the University will endeavor to maximize control of access to buildings and other facilities, it is the responsibility of University Campus Public Safety Office (CPSO) to determine the mechanism used. It is the responsibility of each unit or department to determine who is entitled to request and obtain access to their respective areas and submit appropriate approvals to CPSO.

B. The overall goal of the physical security and access control policy is to provide a reasonable level of security for the University and, at the same time, allow as much freedom of access as possible to the campus community. While maintaining a welcoming and hospitable campus environment, the University will control access to its facilities in an effort to accomplish the following objectives:

1. promote and maintain the safety and security of University faculty, staff, students and visitors;
2. prevent crime where possible, deter that crime that cannot be prevented, and provide tools and information to support investigations and law enforcement;
3. protect University property and assets commensurate with their value;
4. protect and secure University records;
5. protect the integrity and operation of University systems and related infrastructure;
6. protect the integrity of University research projects; and
7. provide governance for access control, safety, and surveillance decisions during normal day-to-day campus operations, campus construction, and remodeling of campus spaces.

C. The purpose here is to establish policies pertaining to granting Access Devices to University facilities; assign responsibility of authorizing access; and implement procedures for the physical security and control of access that has been granted.

3.102 Scope and Policy Statements

A. This policy is applicable to all University colleges, schools, organizations and departments as well as all users of University facilities and users working on behalf or at the behest of the University. It is applicable to all University used, owned or controlled facilities, rooms, grounds and enclosures.

B. University, college, school, program, organizational and departmental policies, procedures, standards and work instructions are required to comply with this policy, with Federal, State and Local laws as well as with other University, OUS and Oregon State Board of Higher Education policies.

C. The granting of Access Device credentials to University facilities shall be subject to the provisions herein.

D. The Vice President for Finance and Administration or designee may authorize, in writing, brass keys for individuals with an authorized ongoing relationship with the University. The Director of Facilities and Planning (FAP) or designee may authorize, in writing, such brass keys as may be required to be issued to non-University individuals or entities to perform services for the benefit of the University.

E. Access Devices Credentials may be granted to University faculty, staff, students, and to non-University individuals or entities authorized access to University facilities.

F. Access may be implemented by the issuance of brass key, fob, code, card, or other Access Device credential, or code.

G. FAP shall retain ownership of all brass keys and be the sole source for the manufacturing, cutting, duplication and issuance and return of all brass keys.

H. CPSO shall be the source for Access Device and fob credential access permissions; Housing & Transportation Services shall be the source for tenant access. CPSO shall also be the sole source for access codes.

I. Individuals to whom access to University facilities is granted are prohibited from duplicating issued Access Device Credentials, or from loaning or providing such Access Device Credentials to any other individual.

J. Individuals violating the University physical and access control policy are subject to disciplinary sanctions, as further described under Section 3.108.

K. Any individual issued an Access Device as herein provided accepts the responsibility for promptly notifying his/her immediate supervisor, CPSO, and FAP in the event the Access Device has been lost, stolen, or otherwise misplaced.

L. Any costs associated with compromised building security or access to University properties, such as manufacturing replacement Access Devices or Access Device Credentials, are subject to the University's Schedule of Fine and Fees.

M. Non-University individuals providing emergency services to the University shall contact CPSO for access.

N. All spaces shall be able to be accessed by FAP and/or CPSO for maintenance or emergency needs.

O. This policy shall be reviewed no less than every three years.

3.103 Definitions

A. Access Control Systems. All systems used by University to control, manage and administer access to University buildings, rooms and spaces. Systems include all hardware, firmware, software and campus infrastructure used for access control purposes.

B. Access Device Credentials. Brass keys, ID key cards, fob keys, proximity keys, codes and other access devices that will allow or control entry into University buildings, doors, rooms, etc.

C. Essential and Highly Sensitive Systems. See the PSU Information Security Policy for definition.

D. Facilities. Any University building, room, or area to which access is controlled by a key or other Access Device normally restricting access to same.

E. Information Technology Infrastructure. All Information Technology hardware, firmware, software and network infrastructure required for campus access control system (s).

F. Key. Generally, any access device designed to control access to University Facilities including brass keys, Access Device credentials, or codes. “Brass key” means a physical key made of metal issued by FAP used to open University door locks.

G. University means Portland State University.

H. University Officer means the authorizing authority or their designee.

I. Written Authorization may include the use of electronic formats when approved in advance by the Director of CPSO and the dean or department head of the controlled space.

3.104 Directive, Authority and Jurisdiction

A. For purposes of implementing the provisions of this policy, the President of the University designates the Vice President for Finance and Administration.

B. The Oregon State Board of Higher Education authorizes Portland State University to establish the University Campus Public Safety Office (CPSO) pursuant to ORS 352.385. This policy applies to Portland State University as organized and empowered by ORS Chapters 351 and 352, and is specifically authorized under ORS 351.087 ORS 315.065 and others.

C. All roles, duties and responsibilities, as further described under Sections 3.105, 3.106 and 3.107 of this policy must comply with other laws, rules and policies, as may be required. These include, but are not limited to:

1. the OUS Information Security Policy (OAR 580-055-0000);
2. the PSU Information Security Policy;
3. the USA Patriot Act Section 326 - governs aspects of identity verification. and requires the University to implement a Customer Identification Program (CIP);
4. OAR 584-017-0055 - levies requirements for establishing the identity of candidates for teaching practicum placement; and
5. The Internal Revenue Service (IRS) levies requirements for establishing the identity of any prospective employee. These requirements are embedded in the I9 forms.

3.105 Governance

A. Ownership of Access Devices and Codes: All access devices issued under this policy and patents to key ways are the property of the University.

B. Administration of Access Control Systems: CPSO is responsible for overall administration and oversight of access and security for all University facilities. CPSO may delegate some or all of this responsibility to other campus departments to accommodate specific access needs or unique situations that may warrant such delegation. All delegations by CPSO shall be in written form describing the specific nature of the delegated authority. CPSO will review the access control decisions for crime prevention and regulatory purposes. CPSO will convene a Physical Security Advisory Committee as needed.

C. Installation and Modification of Access Control Doors, Cameras, Sensors, and Locking Devices: FAP is designated responsibility for all installations or modifications of access control doors, keys, cameras, sensors, and locking devices. FAP, along with CPSO and the Office of Information Technology (OIT), will develop standards, processes and procedures to ensure that consistent access control decisions are made during planning, implementation, and modification of the above, regarding legal and regulatory requirements, crime prevention, security, safety, accountability, adherence to appropriate campus standards (see "PSU ACCESS CONTROL SYSTEM INSTALLATION STANDARDS & REQUIREMENTS – January 2011"), and the efficient flow of traffic.

D. Management of Information Technology Infrastructure: OIT is designated responsibility for management and oversight of all IT infrastructure related to access control.

E. Issuance of Identification (ID) Card Services: Business Affairs Office (BAO) is designated responsibility for issuing ID cards.

F. Designation of Access Control Systems & Infrastructure: Access control systems and associated infrastructure are designated essential and highly sensitive systems. All such systems must be managed and aggregated by CPSO, OIT and FAP.

G. Central Access Control Policy & Procedure Files: CPSO shall establish and maintain a central filing system for copies of all delegated authority and operational procedures documents required under this policy.

3.106 Parameters & Guidelines for Operational Procedures

A. Pursuant to the governance responsibilities as defined in 3.105, above, CPSO, ID Services (BAO), Transportation and Parking Services (TAPS), OIT, and FAP shall develop operational procedures that address accountability and enforce internal controls related to access control, such as required scrutiny during identification (ID) verification, formal processes for granting or revoking access, required record keeping for audit purposes, required deposits, fees and fines, etc. This procedures development requirement shall also apply to all departments granted delegated authority by CPSO under 3.105, above. Additionally, all written delegated authority granted by CPSO shall further detail all applicable procedural requirements of the delegate.

B. These operational procedures must meet the requirements for essential or highly sensitive systems in the University Information Security Policy.

C. Individuals that have the ability to grant access cannot grant themselves access.

D. All persons requesting after-hours access must carry official identification (University ID card or other government issued photo identification).

E. Access control devices without photo ID capabilities must be limited to non-sensitive locations.

3.107 Resolution of Access Control/Security System Issues

A. It is the intent of CPSO to resolve issues in an efficient, cost effective, and friendly manner. CPSO will immediately contact the appropriate Access Authorities and apprise them of any concerns and will assist them in quickly resolving issues.

B. CPSO shall develop, publish and maintain procedures for responding to access related violations or issues with the access control systems.

C. The Chief of CPSO and Chief Information Officer (CIO) shall have the authority to enact and enforce reasonable rules, rates and operations for this policy.

3.108 Sanctions for Non-Compliance

A. The University reserves the right to impose reasonable sanctions, including disciplinary actions upon individuals or departments violating this policy. CPSO will work with the Dean of Students, FAP, HR, BAO, General Counsel, and the Provost's office to develop and implement these sanctions.

B. Brass keys are the property of FAP and may not be retained by individuals or their organization after the date of expiration. All other Access Device credentials are the property of CPSO. Brass keys assigned to faculty, staff, students and designated non-University individuals must be returned to FAP when they have no further official use for the key (i.e. lock changed, door removed, transfer within or separation from the University) or, when their contract expires. All other Access Device Credentials are to be returned to CPSO. In the event of an unreturned Access Device Credential, the individual's organization may be liable for the costs related to restoring security to the area. Fees shall be assessed as described in the University's Schedule of Fines and Fees.