HUMBOLDT STATE UNIVERSITY

Key & Access Control
Policy # TBA (Draft)

Facilities Management

Applies to: This policy applies to all HSU faculty, staff, **students**, **student employees**, contractors, volunteers, and any other individual issued an HSU **access credential**. The policy outlines the responsibilities of **Department**, **MBU**, and **Division Leads** in approving and regulating **access** to University facilities. Any exceptions to this policy can only be made at the behest of the University President or designee. Housing & Residence Life Key Procedures are guided by the Key & Access Control Policy.

Supersedes: University Management Letter 96-1 (2/13/96), Humboldt State University Key Policy.

Purpose of the Policy:

The policy on access credential issuance supports a regulated system of access to provide security for University facilities, assets, as well as the safety of all those on campus. The policy establishes responsibility for all to whom **metal keys**, **key cards**, or any type of access credentials are issued. The HSU Lockshop does not track lockable file cabinets, desk keys, or non-university padlocks. The regulation of such is not included herein. This policy also outlines the individual responsibilities in approving and regulating access to University facilities.

This policy is issued under the authority of Title 5, Part V, Chapter 1, Subchapter 5 of the California Education Code and amendments and additions to Article 9, related to the use of State University buildings and grounds and pursuant to the authority of the President of Humboldt State University for the general welfare of the campus. Unauthorized possession of university access credentials or duplication of university access credentials is strictly prohibited and a misdemeanor covered by California penal code 469.

Definitions

Access – Method of entry to a physical space on campus that is restricted to certain individuals either on a permanent basis or during certain hours of the day.

Access Credential - Key, key card, phone app, **fob**, access code, or any authorized device that gives access to a space.

All School - Spaces that are not allocated to specific departments, but rather are allocated to the entire University. Such spaces include: Restrooms, hallways, stairwells, entryways, some lecture classrooms, and some conference rooms.

Audit Trail - Documentation establishing access credentials assigned to individuals used at a particular time and place.

Building Master - Access credentials that work all the door locks in a building.

Card owner – An individual that has been issued a Humboldt State University key card credential.

Change Key - A single access credential that works a single lock.

Department – Represents a meaningful activity or function within the campus organizational structures. Identifies the "Who": Who is being charged or responsible for the transaction? (e.g. Biology, Learning Center, Registrar's Office). Departments roll up to Major Budget Units (MBUs), which roll up to Divisions.

Department Lead - Hiring authority for a department; typically the Department Chair or Director.

Department Master - access credential that works all locks in a particular department, such as English.

Division - An organizational unit comprised of various Major Budget Units (MBUs).

Division Lead - Hiring authority for a division ; typically the Vice Presidents (VP)

Employee – A person employed by California State University, Humboldt or one of its recognized auxiliary organizations. This individual has a Campus ID number.

Floor Master - A sub master that works all door locks on a building floor.

Great Grand Master - Access credential that accesses all locks of similar type (e.g. electronic, hard key, etc.) except secured spaces.
Human Resources - Department within Administrative Affairs responsible for hiring and terminating personnel.

Key Advisor – A person designated by a Department Lead (i.e. Chair or Manager) as a shared authority for the approval of access credentials to facilities allocated to that department. This role traditionally submits TNS (Telecommunication Network Services) update requests as well.

Key Card – A credential that allows access to spaced via electronic locks.

Key Fob – A credential that allows access to spaces via proximity or at a button press.

Key Holder – An individual issued any form of credential.

Key Watcher - KeyWatcher is a brand name for an electronic key tracking box. Users can be granted access to remove keys that they are approved for. Access is through a User ID and a Pin, there are different levels of access and time periods for having the keys checked out. Keys can be restricted to one or a few users or to many. There are many alarms and warnings that let the department know when keys are not returned, if the box is left open, or if the key is inserted incorrectly.

Lock Box – A controlled storage box, permanently affixed in some manner as approved by the University Lockshop for the storage of credentials to be shared by multiple users within a campus department or departments. A KeyWatcher is a type of lock box.

Master - Access credentials that work multiple doors or multiple locks.

MBU - A reporting mechanism that signifies a major unit, such as a college, within a divisional structure and includes one or more departments. It allows for tracking and reporting at a more summarized level than the department level. (e.g. Facilities Management, College of Professional Studies, Information Technology Services)

MBU Lead - Hiring authority for a Major Budget Unit; typically a Dean or Associate Vice President (AVP)

Metal Key – A credential which is a physical metal key.

Non-Employee – Any individual not possessing a campus ID number. Examples include, but are not limited to vendors, contractors, and visiting scholars.

Person of Interest – An individual who is not an **employee** or student, but is issued a Campus ID number for the purpose of using campus services. Examples include new hires, visiting scholars, and others.

Risk Management - Department within Administrative Affairs responsible for identifying and assessing all types of risk to the campus.

Secured Space - A campus physical space for which all access needs to be explicitly authorized, and therefore cannot be accessed with a campus master key. (See Secured Space Access Common Procedures referenced at the bottom of this document.)

Security Services Grand Master (SSGM) - Key card that accesses all electronics locks on campus.

Student – An individual who is currently enrolled in classes at the university and not employed by the university or one of its auxiliary organizations.

Student Employee – An individual who is enrolled in classes at the university and is employed by the university or a recognized auxiliary organization in the student assistant, graduate assistant, teaching associate, or any student assistant job classification.

Sub Master - Access credential that works several doors but not all doors in a building.

UPD - University Police Department

Volunteer – An individual registered with the Department of Human Resources or Faculty Affairs as an official volunteer for HSU or associated auxiliaries. If this individual needs access to campus spaces, then a campus ID number will be issued. This individual is expected to comply with all relevant aspects of this policy.

Policy Details

<u>Building Hours and Facility Access</u>

University buildings are unlocked and locked in accordance with the schedule published on the Facilities Management Website. If a room is locked during building open hours, someone from the department has deemed it necessary to secure the room.

Facility Management workers shall not unlock offices or other restricted-access areas except in the case of a facilities related emergency or business need. To unlock these rooms, contact the department that manages the area or request access via University Police Department (**UPD**). The UPD Officer will request a photo ID when responding to requests to open spaces and follow internal UPD procedures to verify space allocation and occupancy, which relates to business need and access.

Audit Trails of electronic locks will only be made available by a request from the University President, UPD, HR, or the Facilities Management AVP. Additional requests for audit trail information may be made to UPD or HR and handled on a case-by-case basis. Housing requires a request to be signed by the Director(s) or AVP of Student Success.

Access Credential Requests

The Department **Key Advisor** shall request access credentials on behalf of faculty, staff, students, contractors, or **volunteers**. Access credential requests shall be submitted at least two weeks in advance of expected pickup.

Approval Structure

Each Department Lead (or designee) is responsible for determining and approving access needs for individual staff, faculty, students, student employees, or volunteers to department-allocated spaces.

Access to University facilities is based on an evaluation of the potential **key holder**'s business purpose for access to a particular building, facility, or space. Department Lead (or designee) are responsible for approving access requests to spaces allocated to their Department. Facilities Management shall approve access requests to facilities allocated as "All School" and not to a particular Department. This includes requests for access to temporary structures or short term campus authorized events.

All access credential requests will be approved by the appropriate authority. If that authority is not available within a reasonable timeframe (see Facilities Management Key Procedure for definition of "reasonable timeframe"), the next higher authority in the Department, MBU, or Division will authorize requests. Any exceptions to the Key &

Access Control Policy must be approved by the President of the University or designee in writing.

Certain spaces or high-level access credentials (e.g. Grand Masters) may require multiple levels of approval, including multiple Department/MBU/Division Leads. A written justification statement explaining access need must be submitted along with the access request for higher level access credentials. The tiered approval structure for higher level access is as follows:

Change key, department & sub master: Department Lead
Floor Master: Department Lead & MBU Lead
Building Master: Department Lead, MBU Lead, & Division Lead
SSGM / Grand Master: Department Lead, MBU Lead, Division Lead, & University President. *Issued only in special circumstances.*
Secure Space Access Credential: Secure Space Steward (See Secured Space Access Common Procedures referenced at the bottom of this document.)

Access Credential Issuance

Issued access credentials must be picked up and signed for by the individual to whom the credentials are issued. Access credentials may be issued to departments for check out temporary use if they are kept in a secure key storage location (see "**Lock Box**" below) and audited annually. Temporary use is defined in this instance as no longer than one semester. No Building masters or sub-masters will be included in lock boxes.

Requested access credentials will be held at the Facilities Management front desk (and for Housing, at the Housing Cashier office) up to ninety days for pickup. The requester will be notified that the credentials have not been picked up after 30 days, and again after 60 days of the key being ready for pickup. After ninety days, the credentials will be returned to the lock shop and put back into inventory. Access credentials that have not been picked up within ninety days will trigger notification to the appropriate administrator and may require additional approval for future requests from the requesting department. If the person needs the access credential after this ninety-day hold period, a new request must be submitted by the department Key Advisor.

Any person who has an overdue access credential that has not been returned will not be issued any further credentials until the overdue credential is returned or an extension request is submitted.

Revoking Access Credentials

Any Department granting access to department-allocated spaces may request removal of said access at any time, for any reason. Such revocation may also be requested by the Facilities Management AVP, Human Resources, UPD, or the University President. The maximum active time for any credential will be determined by Facilities Management, based partly on the nature of the credential, and published on the Facilities Management website.

Access Credential Returns

University access credentials are state property and must be returned on demand by authorized administrators. When separating from the University, an employee must request a Separating Access Credential Report from Facilities Management twenty-four hours in advance. All access credentials must be returned to Facilities Management. A receipt will be given listing all access credentials to be returned.

In the case of involuntary separation, Human Resources must request a Separating Access Credential Report prior to notifying the employee so that Human Resources can retrieve all currently issued access credentials (See Separating Employee Clearance Form in References below).

An employee or volunteer may have others return access credentials on their behalf, but the responsibility for these credentials remains with the employee to which the credentials were issued until the credentials are successfully returned. Employees and/or volunteers shall not “exchange” access credentials when changing duties on campus.

Departments are ultimately responsible for all access credentials not returned by faculty, staff, volunteers and students along with any associated costs of re-keying if determined necessary by Facilities Management, **Risk Management**, and UPD.

Students and student employees have an automatic access credential expiration or return date. On that date, electronic access will be automatically revoked and an email will be sent to the student & the department instructing the return of all access credentials. If the individual needs access to be extended, such shall be requested by the Department Key Advisor validating business needs to that space.

Lost/Stolen Access Credentials

Lost or stolen access credentials must be reported to UPD and Facilities Management within twenty-four hours. The sponsoring department must also be contacted with this information. Lost or stolen access credential notifications must be submitted even if the credential will not be replaced. Departments will emphasize the importance of reporting lost or stolen access credentials to individual access credential holders, and work to minimize disbursement of master access credentials. .

Replacement access credentials will only be issued once a Lost Access Credential Request has been sent to Facilities Management and the department has indicated that a new access credential is needed. Facilities Management will track Lost/Stolen Keys and highlight repeated offenses for departments. Departments may choose to change their access strategy to address any repeating problems.

Responsibilities of Access Credential Holders

Access credentials are the responsibility of the individual to whom they are issued and shall not be shared with any other person. Loaning and lending of any access credential to another person is prohibited. In instances where individuals need access to a space to which they do not have access credentials, it is recommended that departments use a lockbox (see below) or submit a request in advance to the UPD for that individual to have the space unlocked on their behalf. If employees require access to a space to which they do not have access credentials and have a legitimate business purpose to enter that space, the department controlling the space may grant that access. If the need is present outside of business hours, UPD can be called to request the space be opened on as-needed basis. The UPD will request a photo ID when responding to requests to open spaces.

Possession of unauthorized access credentials or sharing of such is strictly prohibited.

> California Penal Code 469 [presented herein]. “Any person who knowingly makes, duplicates, causes to be duplicated, or uses, or attempts to make, duplicate, cause to be duplicated, or use, or has in his possession any key to a building or other area owned, operated, or controlled by the State of California, any state agency, board, or commission, a county, city, or any public school or community college district without authorization from the person in charge of such building or area or his designated representative and with knowledge of the lack of such authorization is guilty of a misdemeanor.”

Safes, Lock Boxes, and **Key Watchers**

All safes need to be FM-approved and numbered. Facilities Management will issue and service all combination locks on safes.

If a department requires multiple access credentials for access to specific spaces, then a departmental lock box may be installed. Departmental lock boxes must be approved by the University Lockshop and the appropriate division Vice President. Departmental lock boxes must be wall-mounted or otherwise secured to a physical location and not mobile. A lock box's security must be reviewed by the Associate Vice President for Facilities Management or their designee prior to issuance.

All access credentials in lock boxes will be issued to an individual who will be designated as the lock box owner. If that person leaves the university, then a new lock box owner must be designated. Departments are responsible for controlling access to their lock box. It is the responsibility of the lock box owner to control access to the departmental lock box and maintain a log of who may check out access credentials. Access credentials within the Lock Box may only be used by employees, students, and student assistants. Logs will be checked by the University LockSmith (or designee) at least once a year to ensure proper documentation is kept. Lock boxes that are found to be in continued non-compliance with this policy may be removed, thus leaving only individual access credentials available to the department for issuance. Lock box log templates are available on the Facilities Management website.

Issuance of Access Credentials to Non-State Employees or **Non-Employees**

Departments are strongly encouraged to only request access credentials for employees, students, and student employees. If there is a university business purpose for additional access, such as a key for a volunteer or contractor/vendor, this access may be "sponsored" by a University Employee. The access credential will be issued to the sponsor, and noted that a volunteer or contractor/vendor will be using the credential. Volunteer and Contractor/Vendor access requests will be approved by the appropriate administrator, in accordance with the policy above. All volunteers must be registered as such through the campus Risk department.

All access credentials issued to non-employees will have an expiration date, after which, electronic access will be automatically revoked. Access credentials may only be issued to contractors or vendors for the duration of service. If access credential holder needs prolonged access, the Department may request that the end date be extended. Those requesting keys for events organized by off-campus entities must gain access via the

administrator for campus external events. For Housing and Conference Services, requests can be made for the non-HSU employee event organizer via the Housing staff.

History

Issued: TBA
Revised: TBA
Edited: 10/24/2018, 3/28/2019, 9/13/19, 9/27/19, 1/6/20, 1/30/20
Reviewed: TBA

References

- HSU Secure Space Access Common Procedure
- Building Hours - Facilities Management Website
- Separating Employee Clearance Form - Human Resources