Effective: September 2023

Facilities and Campus Services: Key Security

1.0 Purpose

The University of Alaska Anchorage (UAA) is modernizing to emphasize the utilization of electronic card access systems where feasible. This policy is to provide clear requirements for the management and security of physical keys to campus facilities.

This policy applies to the Anchorage campus and any Community Campus as adopted by the Community Campus Director.

2.0 Definitions and Authorities/Responsibilities

Building Manager: The Building Manager is responsible for approving interior building master key requests.

Campus Security Advisory Team (CSAT): This team is made up of representatives of University Police Department (UPD), Information Technology Services (ITS), Environmental Health Safety Risk Management/Emergency Management (EHSRM/EM), and Facilities and Campus Services (FCS). The CSAT is the Administrative authority to interpret and implement the intent of this policy.

Department Director or Dean: Department Director or Dean is financially responsible for lost keys or costs associated with a rekey. Authority to determine who can obtain a departmental master key. Has approval to delegate this authority to another department or college personnel.

EHSRM/EM: UAA Environmental Health Safety Risk Management/Emergency Management. EHSRM/EM Director has co-approval on high-security key requests.

Employee: University employee has a personal responsibility to follow the key policy including:

Lost keys should be reported immediately to the supervisor, UPD, and FCS. Unneeded keys should be returned to the appropriate key control authority. The default authority for all key control is FCS unless delegated to the department.

Exclusive Keyway: This definition may vary by keyway manufacturer, but generally means a keyway locking cylinder and key that are manufactured for one user and can only be copied by that owner or the owner’s representative with specialized, patented equipment. Exclusive keyways are typically patented for a specific time period and may be exclusive only for a certain geographical region.

FCS: UAA Facilities and Campus Services. Associate Vice Chancellor of Facilities and Campus Services (AVC FCS) has co-approval on high-security key requests.

ITS: UAA Information Technology Services. Chief Information Officer (CIO) has co-approval on high-security key requests.

IMT: UAA Incident Management Team

Lock Shop: UAA FCS Lock Shop

Master Key: A key that opens several locks, each of which also has its own key.

Open (Non-Secure) Keyway: A keyway that allows for keys and locks to be purchased, copied, and milled locally without any special restrictions. Some open keyway manufacturers or owners require a letter of authorization for a key to be copied; however, the security of this letter (who writes it, who requires and reviews it) is not reliable.

Restricted Keyway: This definition may vary by keyway manufacturer, but generally means a keyway locking cylinder and key that cannot be purchased at a local hardware store and that require an authorized dealer for purchase of key blanks or key duplication. Typically, registered and contractually licensed locksmiths purchase the "rights" to sell restricted keys and locks. *Restricted keyways* are not as secure as exclusive keyways, but they are typically more affordable. Restricted locks and keys are usually high quality and are more resistant to break-ins than *open keyways*.

Security Key Designation (High, Medium, Low): Designation given to keys to determine level of liability and risk associated with key control management and associated accountabilities.

UPD: UAA University Police Department. University Police Department Chief of Police (UPD Chief) has co-approval on high security key requests.

VCAS: Vice Chancellor Administrative Services. Authority to receive and resolve complaints and appeals related to this policy.

3.0 Policy

3.1 Management of Keys

I. The protection of the equipment, blank key stock, and stored keys is as equally important as the protection of keys themselves. Facilities and Campus Services (FCS) will, in partnership with the University Police Department (UPD) and Risk Management (EHSRM/EM), conduct a yearly review of the physical space and operations surrounding the storage and production of physical keys.

II. The management of keys and the duplication of keys shall be the sole responsibility of FCS.

   a. Key distribution will be provided by the FCS business office.

   b. FCS Business office will confirm employee identification and secure key signature on the key distribution form.

   c. FCS may delegate this authority to departments for doors that are designated as medium or low-risk priority.

III. Annually, Lock Shop will conduct a review of the system that should, at a minimum, include:

a. The elimination of any individuals and reassignment of keys from individuals who no longer require access to certain spaces or who have left the UAA community.

b. Assessment of overdue keys that need to be returned to FCS.

IV. University Affiliates - Key Distribution and Tracking: contractors, vendors, volunteers, and temporary use. University departments may sponsor university affiliates for the purpose of key distribution. The University Department's responsible employee should be the contract manager or person financially responsible for the activities performed by the University affiliate.

a. The University responsible employee shall complete and maintain records for keys distributed to university affiliates using the form provided. Keys shall be accounted for during an audit.

b. Compliance with this policy applies to university affiliates. The departmental sponsor is responsible to secure compliance with this policy.

V. Security Key Designation (High, Medium, Low). Unless otherwise designated, all keys are designated as medium security key(s). Departments may petition to CSAT for keys to have a high or low designation. High level is subject to annual key audit procedures and high accountability for employees and departments who receive high-security key(s). Low-security keys have less oversight of key control and can undergo key transfers at the department level. The CSAT will conduct a review once a year to validate the individuals who are granted extensive access and high-security levels still require the access level they were granted. Additionally, medium and low-security levels will be reviewed regularly through audits of records.

a. High-Security Designation is defined by the following: access to buildings through exterior doors, campus master key, building master key, and rooms designated by departments that require a high level of key control as determined by the campus security advisory team. It is the intent of this policy that departmental delegation for key management to high-security locations will be rare and managed via exception upon approval by the campus security advisory team.

b. Medium Security Designation: The default security level for all areas unless designated as High or Low. Spaces that are sensitive or confidential should remain in this category. Departmental delegation for key management for this category will be managed via exception and upon approval of the campus security advisory team.

c. Low Security Designation: General departmental spaces that include office support materials and equipment. Departmental delegation for key management will be allowed and encouraged for these locations. Departments / Offices can petition the campus security advisory team for this designation.

3.2 Proprietary/ High Security Key Designation: Exterior Doors, Campus/Building Masters, and Other Designated Areas

I. Keys under this category will undergo an annual key control audit to ensure the key control database is accurate and physical keys assigned to designated employees are located.

II. Departments who are authorized to obtain keys in this category will provide a departmental key security plan to the campus security advisory team for approval.

III. Proprietary/High Security doors key requests require a building manager (for building specific key requests) and dean or director level approval and approved by the CSAT.

   a. If the CSAT does not approve of the key request, appeals can be granted through Vice Chancellor of Administrative Services.

3.3 Hardware Requirements

I. FCS will establish the hardware requirements necessary for the campus buildings, keeping in practice with current security safety standards.

II. FCS may establish locations on campus for a key control box to aid in campus departmental access and reduce burden on key control and annual auditing requirements.

3.4 Departmental Responsibilities and Requirements

I. Departments shall not transfer keys between individuals. Key control and tracking shall be maintained by FCS. Exceptions can be made for some departmental spaces who employ a key tracking system. Exceptions will be audited by FCS.

   a. Requirements for delegated departmental key tracking system: Departments shall keep accurate, up-to-date records of individuals who have keys; records shall indicate key number, date of issue, individual’s name, employee ID number, and phone number. Records may be requested at any time by FCS or by UPD.

   b. If the department fails an audit, the key control exception delegation will be revoked and key control will revert to FCS.

II. Lost keys shall be immediately reported to the employee’s supervisor, dean, or director who approved the key request, FCS and UPD. FCS and UPD will document the lost university property per their internal procedures and coordinate with the supervisor to make sure a risk management report is completed.

III. FCS and UPD have the responsibility to address accountability of individuals not adhering to this policy with appropriate conduct referrals. The cost associated with lost keys and rekeying may be the responsibility of the respective department or office. Departmental budget concerns should never prevent the immediate reporting of damaged, lost, or stolen university property. Accountability measures at their discretion include:

   a. Charging departments an administrative fee for keys not returned by departing employees.

   b. Charging departments an administrative fee for lost keys.

c. Charging departments for the cost of rekeying due to lost keys or keys not returned by departing employees.

d. Unauthorized key transfers shall be treated in the same manner as lost keys with the resulting administrative and rekeying and assigning associated costs for rekey to the responsible department.

3.5 Lost Keys

I. It is inevitable that keys will be lost from time to time. It is important to recognize the difference of importance between campus master keys, exterior keys, and office or suite keys. When an incident is immediately reported of a lost key, the Department and employees will not be penalized for a first-time incident. A determination of a campus master key may dictate different responses. Costs associated with rekeying is considered to be a business expense and never punitive.

4.0 Key agreement form (Suggested use by Departmental Employees to ensure contractor/vendor key accountability and responsibility)

KEY AGREEMENT

FOR University Affiliates (Contractors, Vendors, Volunteers, Temporary Use)

Contractor/Vendor/Entity name: ____

Project/Agreement Name: ____

Date: __________________

University

Contract Administrator/Responsible Person: __________________________________

Key Issued: _________________________ Quantity: One(1) Each

The Contractor hereby acknowledges receipt of the above-listed key(s), and agrees as follows:

- The key(s) will not be duplicated and will be returned at the completion of the work.
- If the key(s) are not returned at the completion of the work, the contractor will reimburse the University for all re-keying and/or locksets required to secure the building.
- Final payment will not be approved until the keys are returned, or reimbursement has been received. The University reserves the right to offset any payments due to the contractor for this purpose.

I acknowledge receipt of the above key(s) and agree to the terms under which it is issued.

Contractor's Representative Printed Name: ____

Signed for: ____ Date _____________

Returned by (printed name): ____ Date: _____________

UAA Representative Accepted by (Printed name) ________________________ Date: ____________