Access Approving Authority Training Manual

University of Alaska - Fairbanks

Abstract

The Access Approving Authority (AAA) training manual explains the process and importance of the university access control systems and how to maintain the security and safety of the campus community by ensuring that only authorized individuals have access. This manual outlines the responsibilities of the AAA, including reviewing access requests and approving or denying them based on established criteria. Through this training, AAA's will gain the knowledge and skills necessary to effectively manage access to their areas, ensuring that the university remains secure, adequately protecting its people, property, and assets.

Facilities Services Access Control

uaf-fs-keyshop@alaska.edu

Table of Contents

Introduction: Access Approving Authority Training

Purpose: The purpose of this document is to provide necessary and relevant information to UAF employees acting as Access Approving Authorities for key issue, and to assist them in effectively safeguarding the integrity of UAF's key systems. We want you to understand not only how to get a key or card access granted to a user, but when and why an access request should be granted or denied.

Background Information regarding the campus-wide rekey project:

Since UAF's foundation in 1917, the university has strived to protect its people and property, as well as secure its buildings and spaces. We have a long history of accommodating evolving departmental missions and growth. As times have changed, so too has our focus on increased security, accountability, and accessibility.

The campus rekey project started out as a project to upgrade hardware on failing doors and an effort to bring all UAF doors up to meet standards set forth by the American Disabilities Act (ADA). Between a push from accreditation groups to change how the university handled building security and a significant lost key incident in 2017, the University's best solution was a rekey scenario for the affected areas. At that time, the Chancellor and Vice Chancellor for Administrative Services (VCAS) initiated a call to increase security and reduce the cost of lost key incidents. In late 2017, it was determined the best course of action was to initiate a full campus-wide rekey, to update building hardware, effectively manage building security, and provide access accountability.

With effective management, a keying system is expected to last ten to fifteen years in an academic or commercial setting, or eight to ten years in a residence life environment. UAF currently has over 20 different keying systems in use, some of which are over fifty years old. The rekey plan is to replace these 20+ obsolete keying systems with one modern, patented system which is protected from unauthorized duplication and designed and scaled for our buildings, departments, and usage. The system is specifically designed to expand as needed, and will allow for easier recovery from lost-key events. This new system reduces the cost for maintenance and operations, improves campus security, and decreases the cost of lost-key incidents.

The nature of UAF's new system is fundamentally different from our previous piecemeal systems as it is designed from the ground up to be a campus-wide system grouped by building and department. This design eliminates many of the security deficiencies associated with our current systems, most of which are obsolete and records-deficient. The new system is also paired with a web-based key management system allowing for on-line requests and approvals while utilizing Banner data and Facilities Services work order system information to reduce response time to requests.

By focusing on Department-level rather than Building-level keys, it may be necessary for some individuals to carry more keys than they did under the previous systems. However, most of the new keys will be a lower security level and if lost will have less impact on the new key system, protecting the system for longer and significantly reducing the cost to individuals and departments.

Access Control Basics:

What is an Access Approving Authority? – A person responsible for controlling who can gain access to the areas under their administrative control. The Access Approving Authority (AAA) is also an information provider, facilitator, and front-line guardian of University spaces. Administrative heads are the default Access Approving Authority for areas under their administration. Default AAA's may designate one or more additional individuals within their department(s) as additional Access Approving Authorities.

A major change with the new key system/software is that the appropriate AAA will be responsible for making all the access requests for access for their area via the new Simple K software. Previously, anyone was able to make requests and only required the AAA for approvals/key slips. The new request process is much easier, no longer requires paper forms, and provides a current status of requests and reporting features.

It is important to note, as an AAA, you will **NOT** need to determine which key(s) to request. Facilities Services Key Shop, working with you and the building users, will determine the type of access needed and will issue all keys, card access, and/or pins (collectively known as "Keys"). You **WILL** need to determine the building(s) and room(s) or door(s) which the requestor has permission to access. If the door is on the card access system, access may be requested by an email from your University email account to the FS Key Shop.

The FS Key Shop will determine the best key(s) and/or access level(s) to grant these requests. In many cases, the FS Key Shop will contact you for more information and seek greater detail in determining the best access for the situation. The Facilities Services Key Shop will work with the AAA (that's you!) to determine the lowest level, lowest risk key that can be issued in each request. **All Keys are the property of UAF and may only be issued by UAF. The UAF Key Shop can be reached at 474-6778**.

The Concept of Least Privilege: The concept of least privilege is a security principle that restricts user access rights to the minimum necessary to perform their tasks. This principle is based on the idea that users should only have access to the resources and data they need to perform their specific job functions, and nothing more.

By limiting access to only what is necessary, the least privilege principle helps reduce the risk of unauthorized access, data breaches, and other security threats. This

approach also helps minimize the impact of a potential security breach, as the attacker would only have access to a limited set of resources.

As part of updating the University's overall security plan, we continue to implement this least privilege principle. This means regular access reviews should be conducted to ensure that users have only the necessary permissions for their roles. Access controls should also be implemented to restrict access to sensitive data and systems. Some computer monitoring and logging tools are in place to help detect any unauthorized access attempts.

Overall the concept of least privilege is an important security principle that can help the University reduce the risk of security breaches and protect their people, sensitive data, and resources.

As an Access Approving Authority, we ask that you keep this principle in mind when making requests on behalf of your unit's users.

Definitions of Relevant Terms

AAA: Abbreviated form of Access Approving Authority, person responsible for determining what spaces a Keyholder needs access to and requesting that access.

Access Review Board: Panel of evaluators for high level key requests created to help centralize and standardize the decision-making process ensuring policy enforcement consistency and system-wide accountability. Made up of the Associate Vice Chancellor of Facilities Services (AVCFS), a University Police Department representative, an Environmental Health, Safety, and Risk Management representative, and an appropriate representative or department head of the requesting department. This independent board will review the need, risk, and necessary precautions associated with restricted access requests in an effort to maintain the integrity of the access control system and appropriate area security envelope, reducing the expense, incidence, and impact of lost key events.

Access Security Plan: Plan developed by each department to address how they will address access security pertaining to their operations. A Unit's Access Security Plan must meet the minimum standard established by the UAF key policy, but MAY be more restrictive depending on each unit's operational needs. This plan will be reviewed by the Access Review Board as part of the decision process for issuing any restricted keys.

Building Master Key: There can be multiple levels of Master Keys depending on the design of the system. A few examples of these varying levels of Master in UAF's key system are:

- Any Key that will open more than one department in a building.
- Key that allows access to ALL dormitory rooms on campus.

- Key that allows access to ALL family housing apartments.
- Other keys that by design will open doors in multiple buildings (such as ALL janitorial closets or ALL mechanical rooms on campus).

Master Keys are the highest level of key available to non-emergency personnel and pose the greatest risk and impact to the key system if lost. A building master key fits all locks in a building and therefore, when lost, affects ALL locks in the system design (physically installed or not) and immediately invalidates 25%-33% of the entire system's key combinations - as a result, thousands of active and unused combinations go in the trash. The graphic below illustrates the hierarchy of key "level". Any change to or loss of a key affects ALL keys below it:

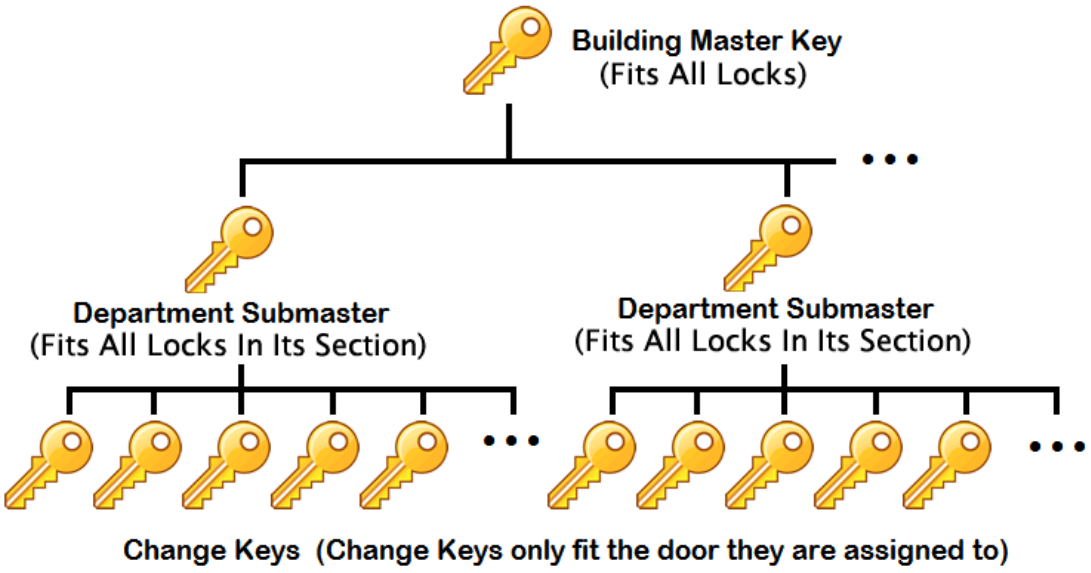

FIGURE 1 - KEY SYSTEM HIEREARCHY EXAMPLE

Change key: (also known as an CK or operating key) - Lowest level of key and lowest impact to a key system if lost. A change key is a type of key that is designed to only open one lock combination specific to the building system. Locks may be keyed alike, which means they are all configured to be opened by the same type of key. Depending on the design size, there can be anywhere from four (4) to one thousand twenty-four (1024) change keys in a section of a key system. Losing a change key subtracts that key's single combination from the total number of combinations available. The remedy for a lost change key is to change the combination in the core to a new combination from the same section of the key system. In the photo below, you can clearly see the "ridges and valleys" that make up the unique combination for a given key.

FIGURE 2 - A KEY CUT TO A SPECIFIC COMBINATION

Core: A core is the small round or figure eight shaped cylinder that holds the key combination and is directly attached to the lock. The key goes into the core to operate the lock. Please see photo of an interchangeable core similar to UAF's system below:

FIGURE 3 - A KEY CORE

Department Submaster: - Mid-level key and significant risk to key system if lost. A department submaster opens all keys in its section of the key system. Many department sections at UAF are designed to have 256 combinations, meaning a department submaster will open all locations any of those 256 combinations have been installed. If a key of this level is lost, so are ALL the combinations that it would open, meaning the system loses 257 combinations (256 change keys + one submaster combination).

DKIO: Abbreviation for Designated Key Issue Office. Only Facilities Services Key Shop, Residence Life and some rural campus sites are DKIO's and have the power to issue some departmental/site-specific keys independently of Facilities Services.

Key Blank: A key before a “combination” is cut into it. The shape and design of a blank is different for each key system, using different keyways, which is why every key won’t go into every lock. Depending on the complexity of the system, a key blank can cost anywhere from $2-$25 depending on the keyway and a blank needs to be cut with a combination of “peaks” and valleys” before it can be used to operate a lock.

FIGURE 4 - A KEY BLANK

Keys: Collectively refers to all physical metal keys, access cards, and pin codes issued by UAF. All keys are property of UAF and may only be issued by UAF.

Key System: The entirety of all keys that share a key blank. UAF’s key system is unique and proprietary to UAF to ensure the safety and security of our people and spaces, custom designed from the factory to accommodate our buildings and spaces with some reserved space in the system set aside to recover from lost key events. Each building will have a certain number of associated keys, typically with 4 Master level keys, 16-64 submaster level keys, and up to 16,384 change keys.

Keyway: Sometimes thought of as the keyhole, but is really defined by the shape of the profile of the key. Keys from different keyways will not fit in the keyhole and thus can not open the lock. See examples of different keyways below.

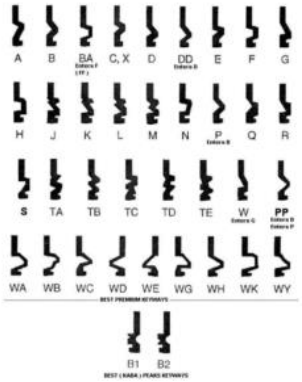

FIGURE 5 - ILLUSTRATION OF VARIOUS KEYWAYS

Simple K: Software used to manage the new key system. Used by AAA's to submit requests and provide reports. Used by Facilities Services to process key requests, accurately manage the database of key information, and provide detailed reports and information. This software allows changes to the key system to be better recorded and implemented at significantly less cost as well as providing a much higher degree of accountability.

Top Master Key: (also known as TMK) Highest level master key, opens all locks in the system. Reserved for emergency / life safety access. The TMK is tightly controlled with extensive security protocols. If lost, eliminates security of all keying in the entire system.

Access Approving Authority Role and Responsibilities:

1. AAA's are responsible for determining who can be issued Keys and/ or have access levels added to their UA ID Card. They are also responsible for submitting access requests to the Facilities Services Key Shop or to other Designated Key Issue Offices as applicable (i.e. Rural Campuses, Remote Research Sites, UAF Residence Life).
2. An AAA may **NOT** request access for themselves. An AAA's key request must be requested by their administrative head.
3. Must follow UAF's Access Control Policy and procedures established by the Designated Key Issue Office they are requesting Keys from.
4. Ensure access requestors are aware of all Keyholder responsibilities and fees associated with lost keys and/or cards as detailed in UAF's Access Control Policy (see Appendix 1)
5. Submit access requests to the Facilities Services Key Shop or to other Designated Key Issue Office via Simple-K software (newly rekeyed buildings) or with the online Key Request Form (if building is still on the older key system(s).
6. Must affirm the requestor's **valid business need** for access and establish the duration access should be granted.
7. Is committing the administrative unit to all costs associated with rekeying university buildings and spaces impacted by Keys lost, stolen, or not returned that were issued with their authority.
8. Is responsible for notifying the appropriate Designated Key Issue Office (usually FS Key Shop) within 30 days when/if a Keyholder is no longer associated with their unit. This includes faculty, staff, and student employees who change jobs within the university or those who permanently leave university employment.
9. **Special note**: FS is in the process of transitioning to a new key system as part of the campus-wide rekeying project. When the new system is fully implemented and the rekeying project is complete (expected 2024-2025), paper key request forms will become obsolete for all key requests. Until that time, online and paper forms may be required for your building.

Determining if an access request should be granted:

Answer the following questions in the grid below. For each space requested, if the answer to **all** questions is YES, proceed with requesting access for the Requestor.

Are you the appropriate Access Approving Authority for the requested space? i.e. you have been designated to approve access for this space.	YES	NO
Does the requestor have a valid business reason to need access to this space? i.e. they require access to these rooms to perform work for UAF.	YES	NO
Have you made the Requestor aware of any safety concerns or additional precautions/training that may pertain to accessing this space? i.e. hazardous materials, special procedures, prior notifications, lab safety training, etc.	YES	NO
Is the requestor aware of all the Keyholder responsibilities for this access? These are detailed in **UAF Key Policy**.	YES	NO
Is the requestor aware of the financial responsibility they are committing themselves and your department to if they were to lose keys accessing the requested spaces?	YES	NO

Key/Alarm Pin Control Procedures:

Requesting key access – What information is needed?:

Information you will need for each request:

- Requestor's name
- Requestor's phone number
- Requestor's email address (UA provided email preferred)
- Requestor's Physical Address
- Department or Contractor name
- Requestor's UAF ID#
- Requestor's affiliation (staff, faculty, student, temp. staff/temp faculty, or contractor)
- Building(s)
- Room number(s) or area

Request Process:

1. If your building is on UAF's new key system, log in to Simple K and complete the request. Or, if your building has not yet been rekeyed, submit electronic Key Request Form @ ***https://facilities.alaska.edu/uaf/fsweb/keyrequest.cfm.***
2. Requests will be verified by email. The FS Key Shop will determine access type and eligibility before releasing the new Keys. Requests are usually completed by the next day**,** but **please allow up to three business days** for Key requests to be processed.

3. When keys are ready, the Keyholder and AAA will be notified by email. Buildings on the new key system will **not** require paper key slips. For buildings on the older key systems, the email will indicate the number of Approver signed paper key slips required.
4. Keys will be issued **ONLY** to the Keyholder named on the key request form. **No one other than the Keyholder may pick up the keys.** A proxy may not be used, and no one, AAA or not, may pick up the keys issued to another individual.

What about Master Keys or Restricted Keys?

In very rare situations, a requestor may request to be issued a Master key or other "restricted" access from you. It's important to understand that an AAA requests and approves access to the ***spaces/doors*** under their control, not the keys. The FS Key Shop will determine the most appropriate key(s)/access level(s) to gain the requested access; however, issuance of some specific Keys/Access levels will require an Access Security Plan as well as an application to and approval from the Access Review Board.

Residence Life - Procedures for requesting Keys from Residence Life, a Designated Key Issue Office, can be found on their website at Residence Life Housing Handbook | Department of Residence Life

Buildings with New Key System - Login to your Simple K account at Facilities Services Simple K Login. Select recipient from drop down menu, enter all request(s) for that individual, selecting which building(s) and door(s) you are requesting access to from the drop-down menus. Click submit.

Buildings with Old key system(s) - Submit an electronic Key Request Form available at Key Request Form on the Facilities Services webpage.

Alarm Pin Numbers - Submit requests for alarm pins to the FS Key Shop via email to uaf-fs-keyshop@alaska.edu, or submit a simple K request with relevant information in the notes field. The FS Key Shop will make the appropriate access assignments and notify you upon completion.

Returning Keys:

IMPORTANT: It is the Keyholder's responsibility to return Keys to the FS Key Shop! The FS Key Shop will provide the Keyholder with a Key Return Receipt as well as confirmation to the AAA if requested.

It is your responsibility as an AAA to make every effort to ensure Keyholders return keys in accordance with University Policy. If efforts fail to have keys returned, they shall be considered lost or stolen, which may require rekeying the affected areas.

Keys shall be returned to the FS Key Shop under **any** of the following conditions:

1. Upon transfer of Keyholder to another department.
2. By last day of employment.
3. By request of the administrative head, site director/manager, AVCFS, or designee.
4. Any disciplinary action that involves a work suspension.
5. Students: At the end of the academic semester or work assignment, when use of Keys will not be required for more than **30** continuous calendar days.
6. Faculty and Staff: When absent for a period exceeding **30** continuous calendar days. However, faculty and staff may retain their Keys if they are authorized to have access to the building and/or place of work (i.e., offices, labs, shops, etc.) during the leave.
7. DD&C Contractors and Consultants: Upon completion of the project with DD&C. FS Key Shop will inform the DDC Project Manager when the Keys are returned so final contract paperwork and payment can be processed.
8. Vendors and Other Non-University Personnel: When the Keys are no longer necessary to complete work. The FS Key Shop will contact the Access Approving Authority when the Key is returned.
9. Space Changes: At the completion of a department moving from one assigned space to another, all Keys accessing the vacated space must be returned to the FS Key Shop by the Keyholders and access levels terminated. The Access Approving Authority will instruct the Keyholders on the requirements to return Keys.

Card Specific Access Control Procedures:

Requesting key access – What information is needed?:

Information you will need for each request:

- Requestor's name
- Requestor's phone number and AFTER HOURS phone number if different.
- Requestor's email address (UA provided email preferred)
- Requestor's Physical Address
- Department or Contractor name
- Requestor's UAF ID#
- Requestor's affiliation (staff, faculty, student, temp. staff/temp faculty, or contractor)
- Building(s)
- Room number(s) or area

Card Access - Submit requests for card access to the FS Key Shop via email to uaf-fs-keyshop@alaska.edu, or submit a simple K request with relevant information in the notes field. The FS Key Shop will make the appropriate access assignments and notify you upon completion.

Access level durations: ALL non-permanent positions MUST specify a duration.

- **Student** access level assignments require an end date at the time of the request. End dates typically correspond to the end of a semester or to the end dates listed in a student employee's contract letter. The maximum length of time for a student access level is **ONE YEAR**. Access may be renewed annually if it is still needed.
- **Graduate Students** - While their duties vary, and they usually have increased privileges, they are still students and their access may be assigned for a maximum of **ONE YEAR** – access may be renewed annually as needed. It is recommended that AAA's request the expiration date of an access assignment to be the following August at the time of request. This will allow AAA's to renew all continuing graduate students access in August simplifying the work load.
- **Temporary Employees** access level assignments require an end date at the time of the request. Their access level end date should correspond to the final date listed in their contract letter or their Service Expiration Date.
- **Permanent Faculty and Staff** access level assignments do NOT require an end date and access will continue until FS Key Shop is notified of a change of status by their AAA, authorizing department, or Human Resources.
- **Vendors, Contractors, Non-affiliated Persons –** If the person has a UA ID, submit the request as above, specifying access – maximum duration without renewal is **ONE YEAR**. If they do not have a UA ID card, contact the Bursar's office for the procedure to have them issued an ID number. Without an ID number, we cannot process access requests for them.

New, custom, or non-standard access levels:

Specific customized electronic access levels to buildings and rooms may also be requested by a department Access Approving Authority. A written request to create or remove access levels for designated areas must be signed by or originate from the Access Approving Authority before submitting the request to the FS Key Shop. An email from your university account is sufficient.

Removing Card Access: To discontinue Card Access, send an email to the FS Key Shop requesting Access Level removal. Please provide:

- Card Holder's Name,
- Card Holder's ID number

- Card Holder’s Department
- Effective date to remove access

AAA’s can do this themselves!

AAAs can request to be authorized to make card access assignments within the Lenel OnGuard software themselves. This enables the department to more nimbly make the card access assignments, while always having the Key Issue office as a backup. AAA’s will need the approval from their administrative head in order to obtain access to the OnGuard software. AAA’s given this software access must comply with all relevant UA and UAF policies and procedures related to access control and information security,

Costs and Impacts

Master keys are higher level keys that open all locks in their section and their loss eliminates all the key combinations opened by that key. Due to key system design, there are typically only four master key possibilities per section, meaning losing a master key twice eliminates ½ the entire system! The best way to protect the system as a whole is to eliminate or seriously restrict access to high level keys and focus on good management of lower level keys.

In past years, many high-level keys were issued for the sake of employee convenience with the expectation that these valuable keys would be safeguarded against loss through an individual's vigilance. Despite everyone's best intentions, some level of loss is inevitable. Accepting that inevitability, the new key system design changes the fundamental philosophy of access control, focusing on reducing personnel access to top level keys, and managing lower level keys with current security protocols. By lowering the security level of keys issued, it is likely that some people may have to carry more keys, but those keys will have less impact and expense if lost, preserving both the security and longevity of the system for as long as possible.

Lost keys above the level of submaster require a rekeying of all doors associated with the Key. The costs for the key(s) will be charged to the Keyholder. The costs for rekeying will be charged to the department that requested the Master key. The risk associated with lost keys at the level of department submaster or change key will be determined by the FS Key Shop in consultation with the authorizing department, and that department will be charged to rekey any doors. Below are several real-world examples of lost keys and the expenses associated with their recovery. These numbers are from actual work order charges from events occurring between 2016-2022.

A. **Lost Change Key** - This is the least impactful loss, removing only a single key combination possibility from the total number available. An example of the costs associated with losing a single change key to a single office, including the replacement of keys and rekeying the lock (if determined necessary) is shown below:

Lost Key Charge to Keyholder (2020)		*$ 50.00*
Labor (2020)	2 hours at $78 per hour =	$ 156.00
Materials		$ 10.00
Total Cost		**$ 216.00**

B. **Lost Departmental Submaster** - This is a significant but recoverable loss. While this loss does permanently remove several hundred key combinations from the system, it only affects 1.5% - 6% of the total combinations available. An example of the costs associated with losing a single Departmental Submaster key to a

single area, including the replacement of all keys and rekeying all locks is shown below:

Lost Key Charge to Keyholder (2020)		*$ 250.00*
Labor (2020)	33 hours at $78 per hour =	$ 2,574.00
Materials		$ 609.86
Total Cost		**$ 3,433.86**

C. **Lost Building Master** - This is considered a major loss. Overall building security and 25% of the building system design would be compromised from this single loss. An example of the costs associated with losing a Duckering Building Master key, including the replacement of all keys and rekeying all locks is shown below:

Lost Key Charge to Keyholder (2015)		*$ 1000.00*
Labor (2015)	162 hours at $78 per hour =	$12,636.00
Materials		$ 91.00
Total Cost		**$ 13,727.00**

D. **Lost Top Master** - This is considered a catastrophic loss. In a situation like this, the possible impact to the safety and security of our students is unacceptable and the damage to the key system shortens the expected lifespan of the system by years, losing 25% of the system per key lost. An example of the costs associated with losing a Residence Life Master key, including the replacement of all Keys and rekeying all locks is shown below:

Lost Key Charge to Keyholder (2020)		*$ 2,500.00*
Labor (2020)	378.25 hours at $78 per hour =	$29,881.75
Materials		$25,806.00
Total Cost		**$55,687.75**

These historical examples above illustrate that the material expense, worker hours, and system impact associated with a lost key event are significantly lessened by lowering the level of the key available. These costs also do NOT reflect the additional time and hassle of re-issuing new keys to all current Keyholders. As materials prices continue to increase – these costs will only go up in the future.

Below is the key schedule with lost key charges detailed by key level.

Lost Key Fee Schedule

Key Level	Approval Authority Required	Lost Key Charge
Top Master – TMK (Police, Fire, UAF Locksmith Access)	Not issued to individuals (AVCFS, UPD, EHSRM, Dept. AVC)	$2500
Building/Utility/Maintenance Master (FS, Janitorial, and CSO Keyrings)	Request through Access Review Board - (AVCFS, UPD, EHSRM, Dept. AVC)	$1000
Department Sub-Master	Access Approving Authority (AAA)	$250
Operating Key or Key Location Device	Access Approving Authority (AAA)	$50