Cornell University

Key Management System

User Manual

August 2009

Version 1.0

Many thanks to the following individuals who were instrumental

in the development of the Key Management System:

Marie Balander, Facilities Services University Lock Shop

Lori Barry, College of Veterinary Medicine

Jocelyn Becraft, Facilities Services

Chris Brown, Cornell Information Technology, Information Services Custom Applications

Greg Busby, Cornell Information Technology, Information Services

Laurie Cecere, Risk Management & Public Safety

Kelly Davis, Facilities Services Building Care

Hugh Edwards, Cornell Information Technology, Information Services Custom Applications

Peggy Emerson, Facilities Services Customer Service

Chris Grippin, Cornell Information Technology, Information Systems

Nancy Kimble, Cornell Information Technology, Information Services Custom Applications

Linda Grace-Kobas, Cornell University Finance & Administration Communications

Juliet Hendricks, Facilities Services Building Care

Jay Hulslander, Cornell Information Technology, Information Services Custom Applications

Kristine Mahoney, College of Human Ecology

Carrie Maine, Facilities Services Building Care

Peggy Matta, Risk Management & Public Safety

Kevin McCord, Facilities Services Customer Service

Rachel Moore, Facilities Services Customer Service

Brenda Payne, College of Veterinary Medicine

Tim Petriwsky, College of Human Ecology

Daneen Phillips, Risk Management & Public Safety

Nancy Preston, Campus Life

Ray Price, Cornell University Police

Joe Remillard, Facilities Services Customer Service

Becky Richmond, Campus Life Multi-Trade Shop

Barb Romano, Campus Life

Brandi Smith, Campus Life

George Sutfin, Cornell University Police

Table of Contents

Key Management System Manual   5   August 2009

Version 1.0

Table of Figures

Overview

Access Control

University Policy 8.4 – Management of Keys and Other Access Control Systems - requires that departments and units maintain control of all devices and systems that provide access to university facilities and vehicles. This includes possession, issuance of copies, and storage of keys and other access devices. In addition, device holders are required to maintain control of access devices issued to them, ensure their proper use, report lost devices, and return devices to their supervisors when no longer required.

Everyone acting on behalf of Cornell University must take responsibility for faculty, staff, and student safety, as well as the security of university physical space and the assets contained therein. An essential element of security is maintaining adequate control to ensure that university assets are accessed only by those authorized to do so. This necessitates the tracking of university key systems and access devices, as well as the locations they access and the individuals to whom they are issued.

Responsibility for the management of proper access control rests with unit heads, who must each designate one access control coordinator (ACC) and/or key control coordinator (KCC) for all functional work areas, or delegate this responsibility to a specific entity within a unit. In all cases, ultimate responsibility for the access devices in a unit rests with the individual to whom the access device was issued.

Issuance of access devices should be systematic and need-based. Immediate supervisors, in consultation with ACCs and/or KCCs and in accordance with this policy, must determine the need for access device issuance, based upon job functions. Issuance of access devices should be kept as infrequent as possible, with consideration given to hours of work, work space, alternatives, frequency, urgency, and sensitivity (see the "Considerations When Issuing an Access Device" segment of this policy).

Immediate supervisors, ACCs, or KCCs must train device holders in the proper use of access devices and review this policy periodically with them.

Any individual requesting access to a space must complete a sign-out procedure with an ACC or KCC, or a designate, when receiving an access device. A responsible party (see "Definitions") must sign out an access device for any person who is not a Cornell student, faculty, or staff member.

Individuals are prohibited from unauthorized possession or duplication of access devices to university facilities or vehicles; from disabling or circumventing access devices; and from making changes to access without following the procedures set forth in this document.

Because all levels of master keys (grand-master, master, sub-master, etc.) open more than one space, additional care must be taken in safeguarding them. Where possible, master keys should be kept in secured storage rather than carried by an individual.   Individuals should carry the lowest level key that meets their business needs.

Key Management System

The Key Management System (KMS) is intended to help users meet the requirements of Policy 8.4 – Management of Keys and Other Access Control Systems for physical keys. The KMS has been designed to meet the following general requirements:

- Capture key profiles

- Establish an organizational structure for managing keys within your unit to include Key Control Coordinator(s) and Associate Key Control Coordinator(s).

- Inventory physical keys, including

    o organizing keys by Key Groups and Key Rings

    o assigning access locations to keys

- Capture transactions associated with keys such as:

    o Assigning keys to individuals

    o Putting keys in storage

    o Identifying a key as lost/stolen or broken

The KMS was designed specifically to meet Cornell's needs and is intended to be flexible to allow for differences in the ways keys are managed within various units. A committed group of stakeholders was involved in the development of the KMS and we hope you find that it can be successfully used to manage your key inventories at Cornell.

Within the year, the KMS will have the ability to print reports to meet the annual review requirements of Policy 8.4. We will add documentation to this manual when that functionality is developed.

We are planning for Phase II of the KMS that will include electronic workflow to allow the requesting of duplicate keys and the associated approval process to happen all on-line. We do not currently have a release date for Phase II.

Definitions

The following definitions are used with the Key Management System and are consistent with Policy 8.4 – Management of Keys and Other Access Control Systems.

Access Device	A mechanical or electronic device, including, but not limited to, a key or an access card, used to gain access to a university facility or vehicle.
Associate Key Control Coordinator	An individual responsible for issuing, receiving, and maintaining key assignments, key inventories, transaction systems, forms, and records, as delegated by the key control coordinator (KCC).
Access Locations	The facility and room(s) that a key can access. This information is linked to the university facilities inventory.
Bitting Notches	The unique cuts made to a physical key.
Change Key	The lowest level of a key system. A change key cannot have any child keys below it.
Children	Keys that are below other keys in a key system. For example, a sub-master would be a child key to a master key.
Due Date	A specific date assigned to a key for verification process and/or turn in date if the key is issued on a temporary basis.
Emergency Access	Access for the purposes of security, law enforcement, human safety, or facility repair.
Emergency Response Personnel	Individuals assigned access devices that allow emergency access to a broad number of campus facilities for the purpose of providing emergency services.
Emergency Services KCC	A KCC that can make instances from any key profile in the KMS, after approval from the Cornell University Police, with the exception of secured keys. Emergency Services KCCs include the Cornell University Police and Environmental Health & Safety.
Key Control Coordinator (KCC)	An individual acting on behalf of the dean or vice president who is responsible for requesting, issuing, receiving, and maintaining key assignments, key inventories, transaction systems, forms, and records. A KCC may delegate authority for a subset of keys to one or more associate key control coordinator(s) (AKCCs).
Key Control Coordinator Back-Up	The individual designated to provide back-up for the KCC. The KCC Back-up can perform the duties of the primary KCC.
Key Instance	An individual physical key.
Key Management System (KMS)	An electronic, online tool available for managing and tracking inventories of physical keys. **Note**: All keys to spaces with special access restrictions (e.g., those with highly hazardous materials or highly valuable assets), must be inventoried in the Key Management System (KMS). Authorization to this system is role specific and must be authorized by the Cornell Police and/or the Key Management System Program Administrator

Key Profile	This is a conceptual entity that represents the common properties that duplicate keys share. For example, you can have many identically duplicate keys, but they would all map back to a single key profile. Access Locations are assigned at the Key Profile level, because duplicate keys would all open the same access locations. A Key Profile is uniquely identified by the combination of manufacturer, keyway, and bitting, and can be referred to by its Key Set.
Key Tag	The identification device with a unique number usually attached to a key ring. Key tags for staff, students or faculty are available from the Cornell University Police in G-2 Barton Hall.
Device Holder	An individual in possession of any physical, electronic, or other access device (may be a university employee, student, volunteer, alumnus, outside vendor, or authorized visitor). For purposes of this manual, the term key holder will be used because this manual is in reference to physical keys.
Key Holder	Per Policy 8.4, this is a device holder that is in possession of a physical key.
Key Ring	A set of keys physically bound on a ring. Key rings are stored or assigned to recipients as a single unit.
Key Sequence	A sequence number assigned to a physical key that differentiates it from other keys of the same cut and key stamp. (e.g., KA1 vs KA2)
Key Set	A series of letters and/or numbers that the key manufacturer and Lock Shop use to uniquely identify a key profile. The Key Set is typically stamped onto the physical key.
Key Stamp	A series of letters and/or numbers stamped onto a physical key for purposes of identification. It may or may not be the Key Set. Combined with the Key Sequence, it should be unique.
Key Way	The grooves cut along the length of a key that determine which keyholes it can be inserted into
Master Key	A key that fits or opens more than one door. There are several levels of master key, each with different capabilities and rules for issuance and use (e.g., master key, sub-master key, grand-master key).
Orphan Key	A Master, SubMaster, or Change key that does not have a parent.
Responsible Party	A Cornell employee responsible for the access devices provided to a person who is not a Cornell student, faculty, or staff member. (e.g., visiting professor)
Secured Key	A key that requires specific approval of the KCC to be duplicated by Emergency Services or Service KCCs.
Service Access	Access for the purposes of providing maintenance, repair, and building care services.
Service KCC	A KCC that can make instances from any key profile in the KMS, after approval from the Cornell University Police, with the exception of secured keys. Service KCCs include Facilities Services Customer Service and Building Care.
Service Personnel	Individuals assigned access control devices that allow service access to a broad number of campus facilities for the purpose of providing maintenance, repair, and building care services.

Special Information	Specific requirements associated with an access location. For example, a room containing highly hazardous materials may require that a specific person approve any keys issued for that room.
Sub-Master Key – see "master key"	
Temporary Access Device	An access device assigned for a limited time.
Unit	A college, department, program, research center, business service center, office, or other operating unit.

Roles and Responsibilities

The following roles and responsibilities are as defined in Policy 8.4 – Management of Keys and Other Access Control Systems.

Access Control Coordinator (ACC) or Key Control Coordinator (KCC)	• Request authorization from the Crime Prevention Unit of the Cornell University Police Department (CUPD) for duplication of keys. • Store, protect, and distribute access devices/systems properly. • Ensure emergency response and service personnel have proper access to facilities and spaces. • Periodically initiate reevaluation of the need for access devices and retrieve them, or the appropriate access, when necessary. • Designate associate access control coordinators (AACCs) or associate key control coordinators (AKCCs). • Receive and act on requests for access devices, and changes to access. • Issue temporary access devices. • Uniquely identify and mark access devices. • Maintain access device records, including associated access locations. • Conduct a review of access devices/systems and associated locations at least every two years.
Associate Access Control Coordinator (AACC) or Associate Key Control Coordinator (AKCC)	• Receive and act on requests for access devices, and changes to access. • Store, protect, and distribute access devices properly. • Maintain an access device record system. • Issue temporary access devices. • Uniquely identify and mark access devices. • Conduct a review of access devices and associated locations as requested by the access control coordinator (ACC) or key control coordinator (KCC).
Campus Card Access Administrator	• Maintain central card access server and database. • Notify users of outages. • Maintain network link to the University Registrar's office. • Administer ACC access rights.

Campus Life Multi-Trade Shop	• Store, protect, distribute, and maintain information pertaining to Campus Life key systems (including bitting numbers, keyways, etc.) in the Key Management System (KMS). • Reproduce Campus Life keys as requested and appropriate, via the Campus Life work-order system, and in accordance with this policy. • Change locks with Campus Life as requested by individual units. • Provide estimates for Campus Life new installations, upgrades, or conversions.
Crime Prevention Unit of the Cornell University Police Department (CUPD)	• Maintain a list of authorized ACCs and KCCs, and their backup(s), AACCs, and AKCCs. • Conduct periodic inspections of the records and facilities for key and access card control. • Forward approved and authorized key requests to the University Lock Shop and the Campus Life Multi-Trade Shop.
Deans, Vice Presidents	• Ensure that the college or unit meets the minimum standards set forth in this policy. • Authorize ACCs and KCCs for the college or unit using the "Access Card and Key Control Authorization Form" (see "Related Documents,

Key Parts

The following diagram represents typical parts of a standard key issued by the university lock shops. See the Definitions above for additional information.

Figure 1 – Key Parts
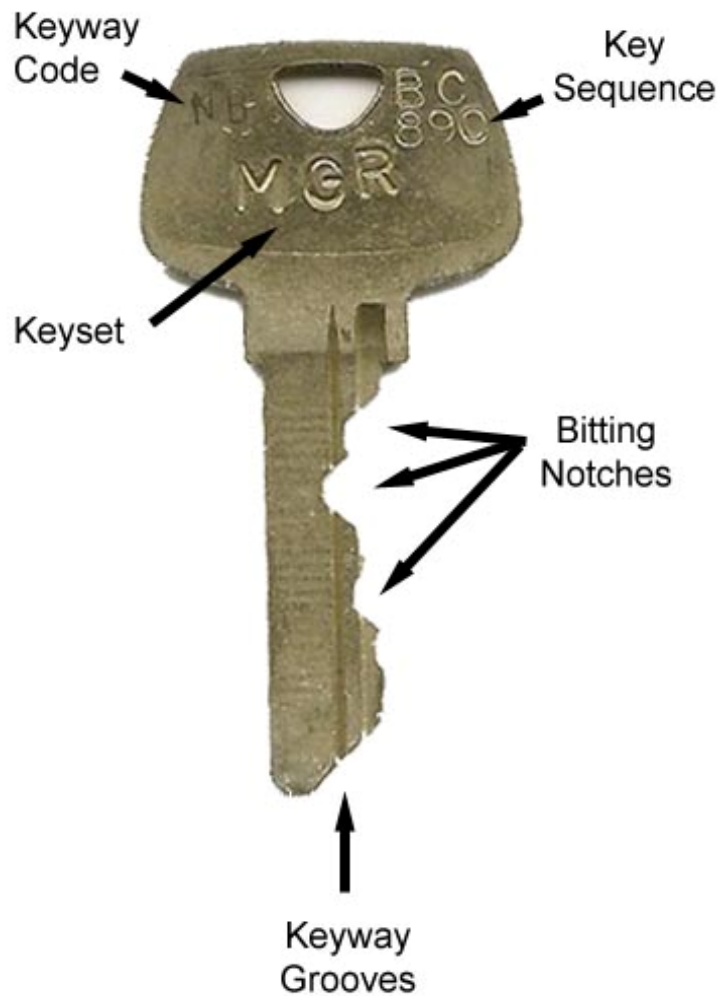
Key "Family" Tree or Profile

The following is a depiction of a key "family" tree. A typical tree goes from Grand Master to Master to Submaster to Change key. Note in the tree below the variations that are possible to a tree. Examples include:

- Change keys off of Grand Master and Master keys, and
- Orphaned keys that aren't related to the rest of the tree.

Figure 2 – Key Profile or "Family Tree"
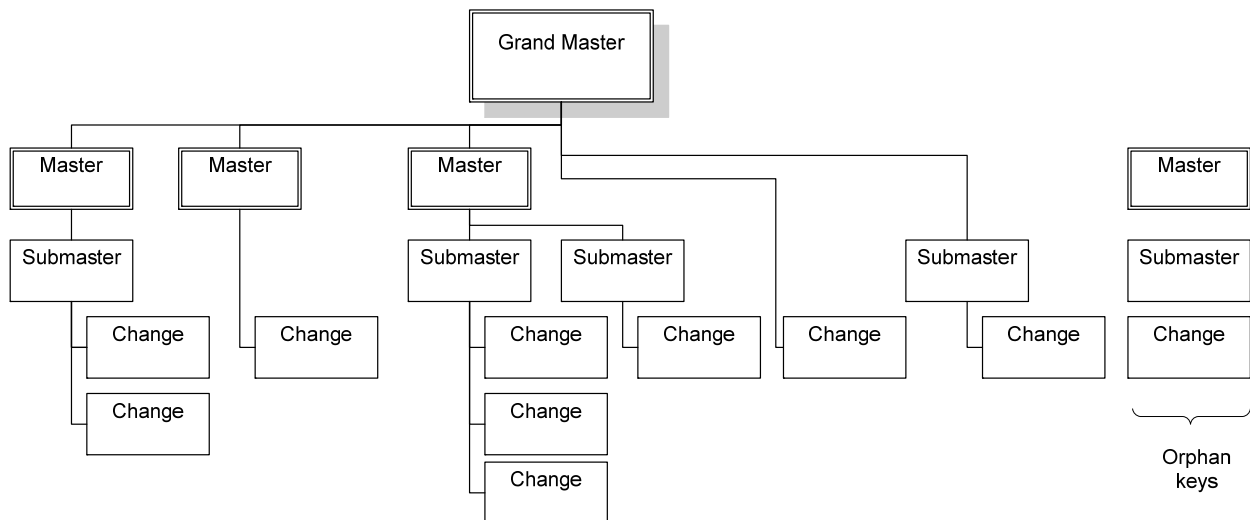
Key Management System Process

The following figure depicts the process that must be followed for a KCC to be able to manage their keys within the KMS.

Figure 3 – Process to Manage Keys within the Key Management System

Lock Shop	KCC	AKCC
1. Create key profiles	2. Assign access locations to key profiles 3. Assign AKCCs 4. Create key groups 5. Create key instances	6. Create key rings 7. Assign keys and key rings 8. Sign keys and rings back in 9. Identify keys as lost/stolen or broken
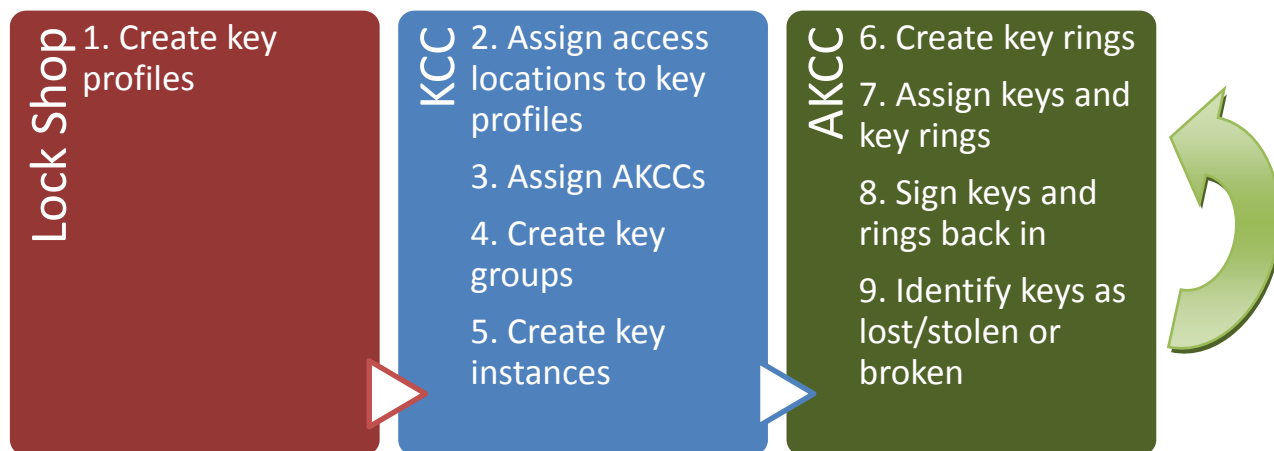
Note that prior to using the KMS, a unit must work with the appropriate Lock Shop to have the key profiles for their facilities entered into the KMS. The University Lock Shop has many key profiles available and depending on the age of the keying system, some profiles may be readily available for conversion into the KMS.

The process defined in Figure 3 above is outlined in considerable detail in the following sections of this manual.

Key Conversion Process

A data conversion process is available for units that put their key inventory information in spreadsheets provided by Risk Management and Public Safety. The conversion process has the ability to pull key profile information and key instance information into the KMS. The conversion process is further defined in

Appendix C – Importing Key Instance Information into the KMS.

Authorization Matrix

The following matrix is provided for general reference and summarizes the possible actions within the Key Management System and which roles are authorized to perform those actions.

Actions	AKCC	KCC	Service & Emergency KCCs	Lock Shop
Manage key rings	X	X	X	
Create a key ring	X	X	X	
Edit a Key ring	X	X	X	
Delete a key ring	X	X	X	
Edit only notes on a key	X	X	X	
View logs	X	X	X	
View special information	X	X	X	
View access locations	X	X	X	X
Manage access locations		X	X	X
Create a key group		X	X	
Add an AKCC		X	X	
Delete an AKCC		X	X	
Add a custom location		X	X	
Edit a custom location		X	X	
View secured profiles		X		
Create a key instance		X	X	
Duplicate a key instance		X	X	
Edit a key instance		X	X	
Insert special information		X	X	
Update special information		X	X	
Create a key profile				X
Edit a Key profile				X
Destroy a key				X

Key Management System

Accessing the Key Management System

The Key Management System contains confidential information. A lot of time and effort has been devoted to ensure that system data and your unit information are safe and secure. Access into the system is highly regulated by the Crime Prevention Section of the Cornell Police Department and the Key Management System Administrator.   Each college/major unit is responsible for the creation and maintenance of key inventories for their individual department/unit(s).

Obtain Authorization as a KCC

Prior to using the KMS, a KCC must be authorized by their Dean or Vice President. Authorization forms are available at: http://rmps.cornell.edu/keysinfo/. The authorization form must be sent to the Cornell Police, Crime Prevention Section, G-2 Barton Hall. Upon receipt of the authorization, the KMS Administrator will provide access privileges to the KCC within the KMS.

To Access the KMS

NOTE: We recommend using Mozilla Firefox. It loads the pages much more quickly than Internet Explorer and displays the system information in a more easily read format.

Use the following URL: http://rmps.cornell.edu/keys/

Immediately after using this link, you will see the first line of security: The CUWebLogin screen. You will be required to type in your netID and password.

RMPS Home Room screen:

If you are not authorized to use the Key Management system, you will not see the Key Management icon Box. If this happens, you should contact the Key Management System Administrator at kmsusers@cornell.edu.

If you are set up in the system, you will see the Key Management system icon.

Click on [icon] to enter the system.

Key Control Coordinator (KCC) Procedures

As KCC you are responsible for the management of keys and key systems data. Management of keys includes: maintaining key inventories and associated storage locations, maintaining transaction logs of all changes in key assignment, processing all required and associated forms, and maintaining all records for your college or major unit.

Figure 4 – KCC Responsibilities within the KMS

Lock Shop
1. Create key profiles

KCC
2. Assign access locations to key profiles
3. Assign AKCCs
4. Create key groups
5. Create key instances

AKCC
6. Create key rings
7. Assign keys and key rings
8. Sign keys and rings back in
9. Identify keys as lost/stolen or broken
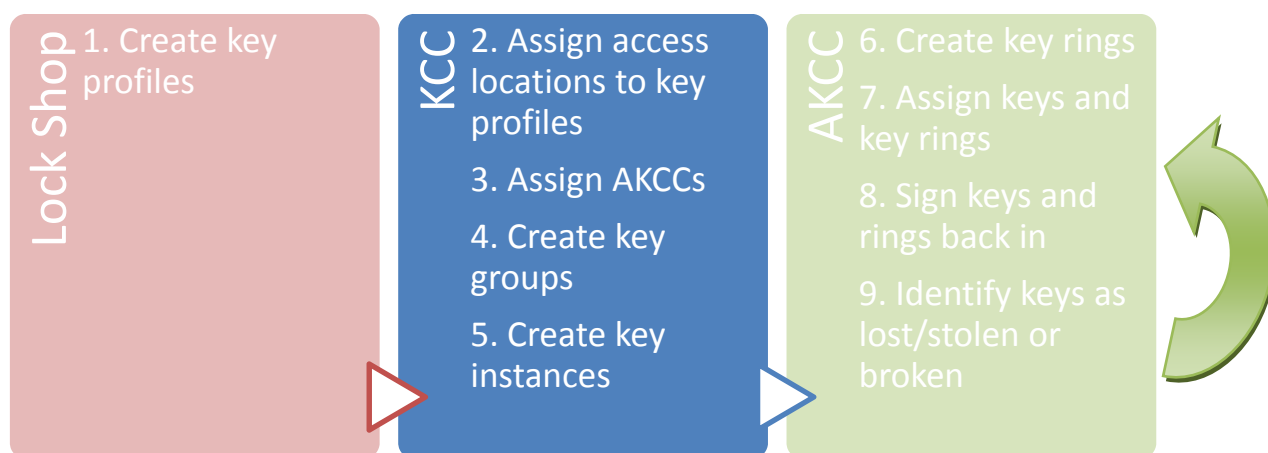
Note: Any of the responsibilities listed above for AKCCs, as well as the actions that an AKCC can perform within the KMS, can also be performed by a KCC.

Get Your Key Profiles Established in the KMS

Prior to being able to use the KMS, the key profiles for keying systems which are installed in facilities for which you occupy and/or are responsible must be entered into the KMS by the appropriate Lock Shop. A key profile is essentially the 'family tree' of a key system. (See Figure 2 – Key Profile or "Family Tree" on page 14.) A profile indicates where in the 'family tree' a specific key instance belongs. A 'key instance' is an individual physical key. Contact the PDC Lock Shop at (x5-7112) or the Campus Life Multi-Trade Shop at (5-2074) to discuss getting your unit's key profiles entered into the KMS.

My Key Profiles

This screen displays a list of all the key profiles for keying systems which are installed in facilities for which you, as the KCC, represent the occupants and/or are responsible for the stewardship. These key profiles are established and assigned by the Lock Shop. (See Get Your Key Profiles Established in the KMS on page 19.)
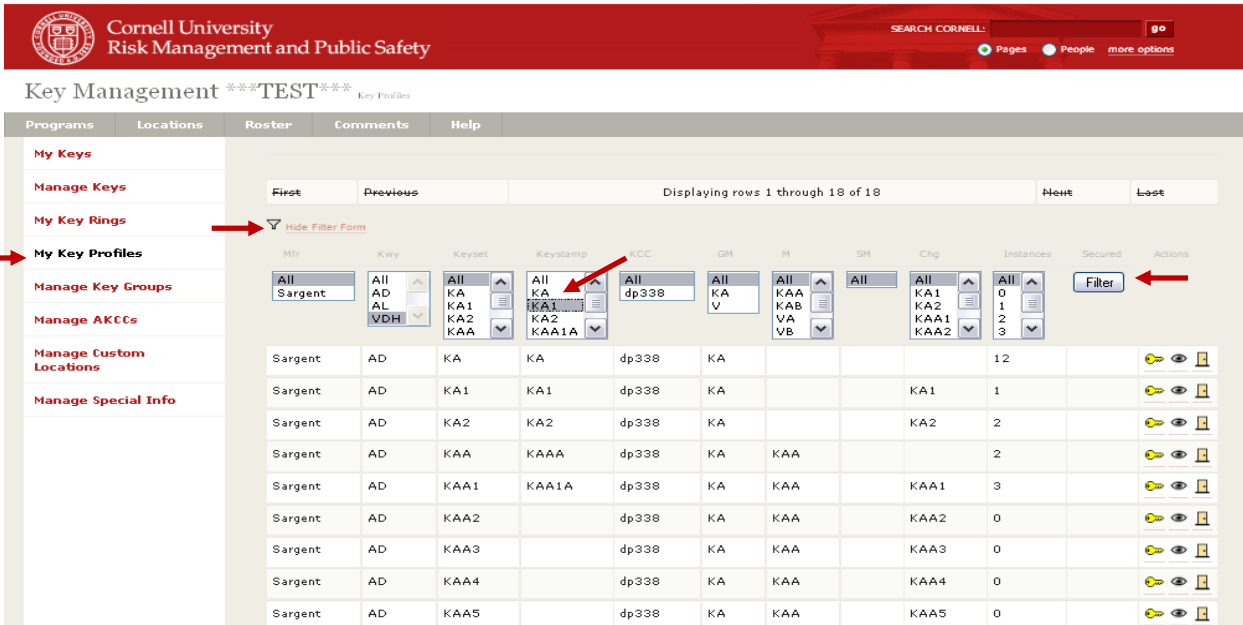
➢ To view all key profiles:
   Use this screen to view keys by key system information such as the manufacturer, keyway, keyset, or key stamp.

   • **Go To** "My Key Profiles".

➢ To filter the view:
   • **Click** ▼, this will open drop down options which allow you to filter the view by any one or more of the following: manufacturer, keyway, keyset, key stamp, grandmaster, master, sub-master, or change.
   • **Click** on the item you wish to filter *(the item will be highlighted.)* Use Shift+Click to select multiple sequential items at one time. Use Ctrl+Click to select multiple non-sequential items within a filter box.
   • **Click** "Filter".

➢ To view a specific key profile:

- **Go To** "My Key Profiles".

- **Click "**View" icon 👁 next to the key profile you wish to view.

- The following screen will open:

  The detail of the selected key profile, as well as the parent and any children profiles associated with the selected profile will be displayed.

➢ To view information about a secure key profile:

When you view My Key Profiles, the "Secured" column denotes keys that have been identified as secured. An emergency response or service KCC cannot make instances of secured keys.
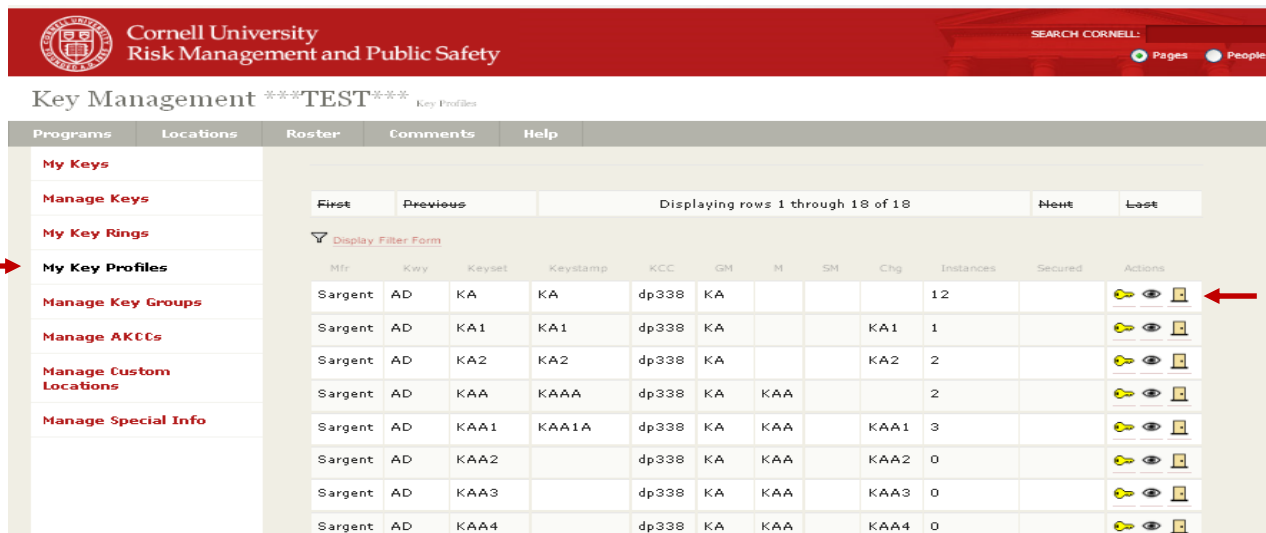
➢ To assign access locations to key profiles:

Once key profiles have been entered into the KMS by the Lock Shop, associated access locations must be assigned to each profile. Both the Lock Shop and the KCC for a key profile have the ability to assign access locations; however, in practice the maintenance and management of this information is the responsibly of the KCC.

Access locations should be assigned at the lowest possible level in a profile. Parent keys inherit the access locations of their children keys. For example, if a change key opens room 100A in Facility X, then

the sub-master, master and grand-master (all parents of the key) will all open door 100A in Facility X. In this case, the access location of room 100A should be entered only once at the change key level.

- **Go To** "My Key Profiles"
- **Click** "Locations" icon ![] at the far right side of the table. This will take you to the locations screen.

- **Enter** the facility code or **choose** the facility from the drop-down list. If you begin to type the numerical sequence of the facility code the list will jump down to the appropriate subset of codes.
- **Enter** the room number or **choose** the room from the drop-down list. If you begin to type the alpha-numerical sequence of the room the list will jump down to the appropriate subset of rooms.
- **Click** "Add Location"
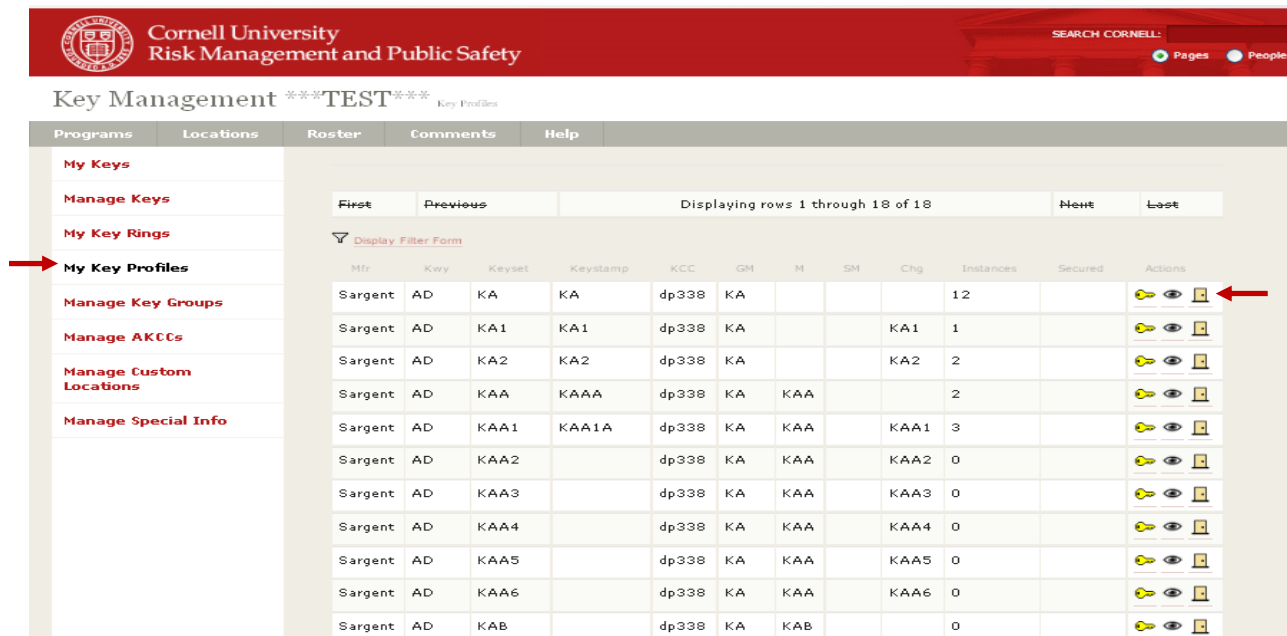
➢ To delete access locations from key profiles:

- **Go To** "My Key Profiles"
- **Click** "Locations" icon at the far right side of the table. This will take you to the locations screen.

- **Refer** to "Current Key" in the "Key Information" area at the top of the screen.
- **Click** "Delete" for the location you wish to remove.
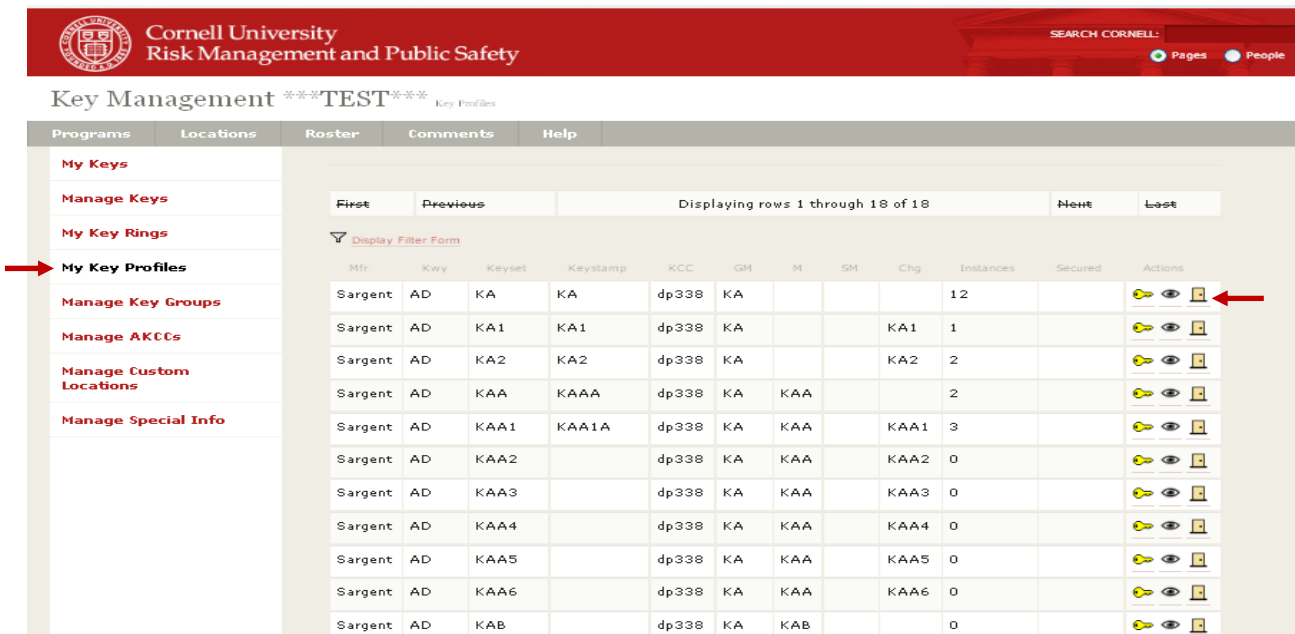
From this screen you can also see the access locations already assigned to this key, any children keys of the current key, and the parent keys of the current key.

➢ To identify access locations with special information:
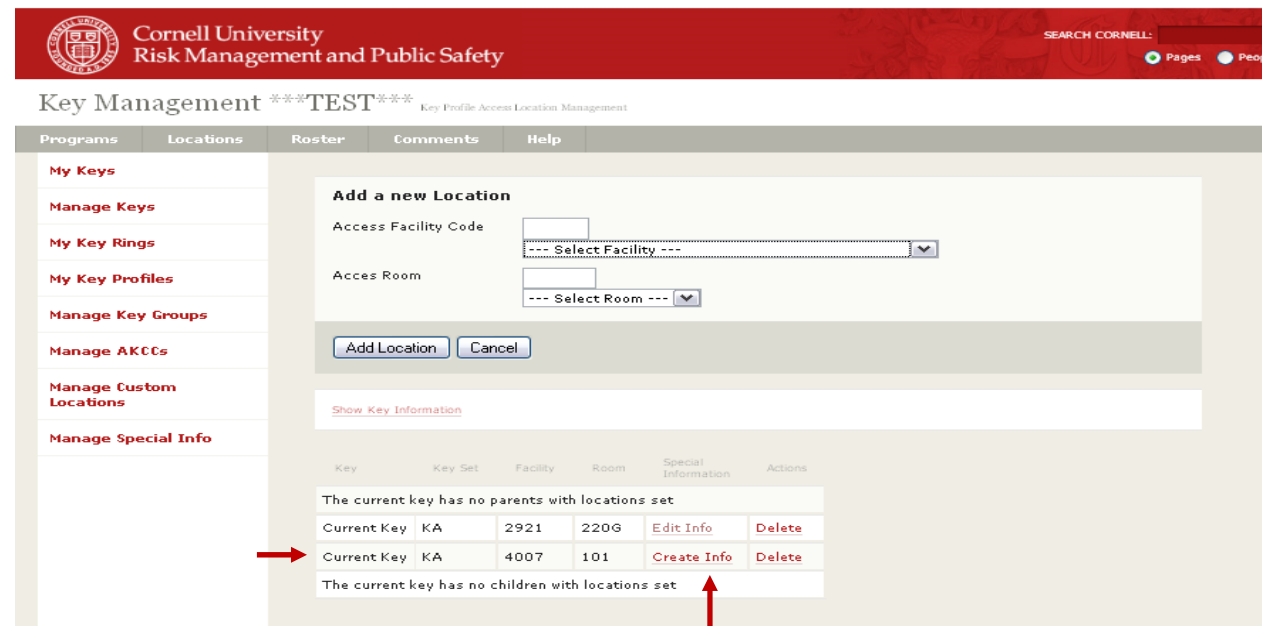
From the same locations screen, you can also edit special information associated with the access locations for the current key or other keys in the profile. For example, a room with highly hazardous materials in it may require that a specific person approve any keys issued for that room.

- **Go To** "My Key Profiles"
- **Click** "Locations" icon ▯ at the far right side of the table. This will take you to the locations screen.

- After you have entered an access location for a key (the step above), **click** "Create Info"

- **Enter** the netid of the approver for access to this space.
- **Enter** any notes that describe the special information.
- **Click** "Create New"
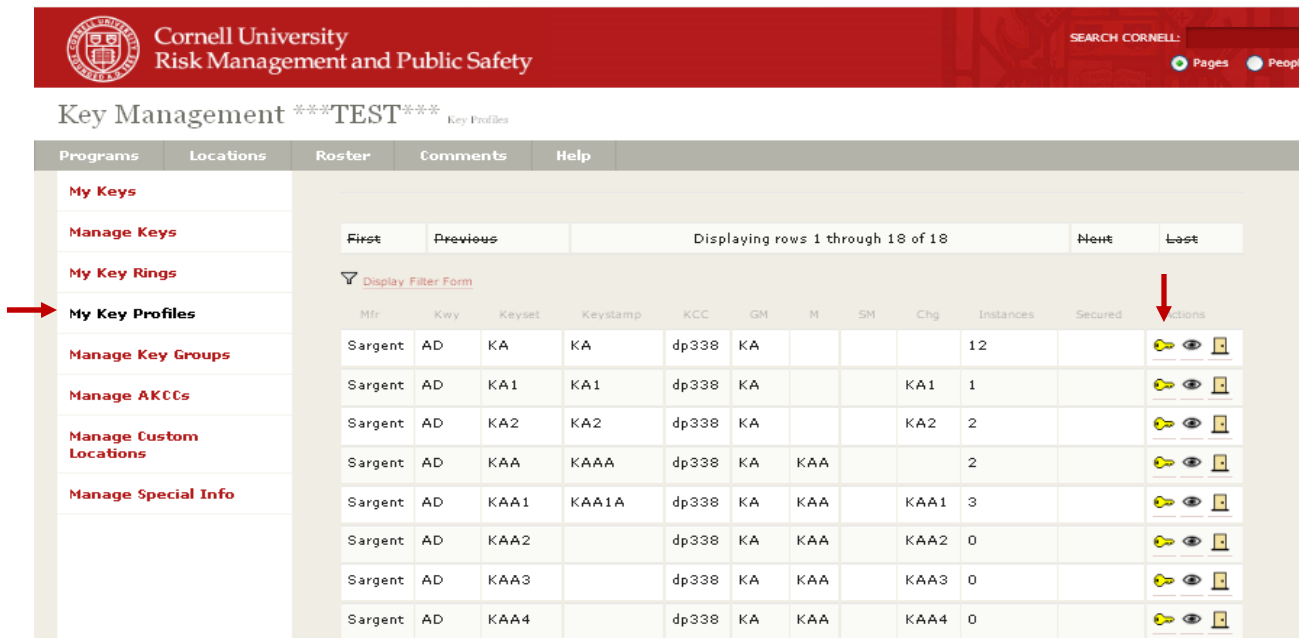
➢ To create a key instance:

    ✓ *To have a new physical key instance made, first complete the University Key Order Form available at www.rmps.cornell.edu/keysinfo. Follow the instructions on the form for approval by the KCC and the Cornell University Police.*

Follow the steps in this section to enter your existing physical key instances into the KMS or to enter new keys instances into the KMS. If your existing key information is available in a database or spreadsheet, it may be easier to import your information into the KMS. See
Appendix C – Importing Key Instance Information into the KMS for more information.

- **Go To** "My Key Profile".
- **Click** "Make Instance" icon ⚿ on the row of the appropriate key profile.

This will take you to the key instance screen for further details.

Key Instance Screen

- **Input** the Key Sequence. This should be a unique value and should be stamped on the key for identification purposes.
- **Choose** the Key Group that this key should belong to from drop down field. (You must first establish Key Groups. See Manage Key Groups for more information.)
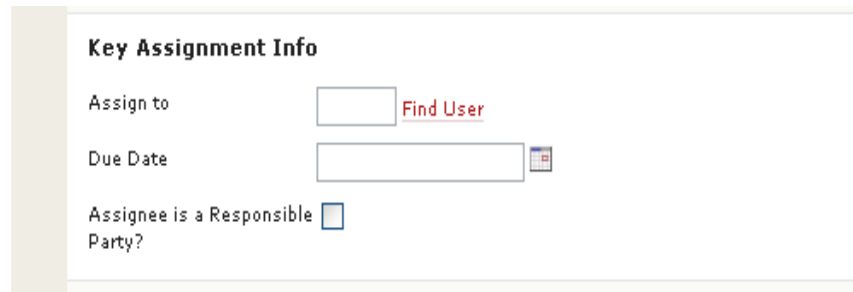- **Choose** a Key Ring, if appropriate, from the drop down field. (You must first create Key Rings. See

- Manage Keys for more information.)
- **Enter** any appropriate notes in the text box. For example, you may want to note why you've created this instance.
- At this point you must either assign the key to a key holder or put the key in storage.

➢ To assign a new key instance to an individual:
In the section Key Assignment Information:

- **Input** the individual's Netid in text box **or** click Find User.
- **Enter** the due date or click [calendar icon] to display a calendar and select the date that the key needs to be returned by. This field is optional.
- **Enter** notes as appropriate.   For example, you may want to note why this key has been issued or based on whose request.
- **Check** the appropriate box if the key is being assigned to a Responsible Party. (See

Definitions for more information about Responsible Parties.)
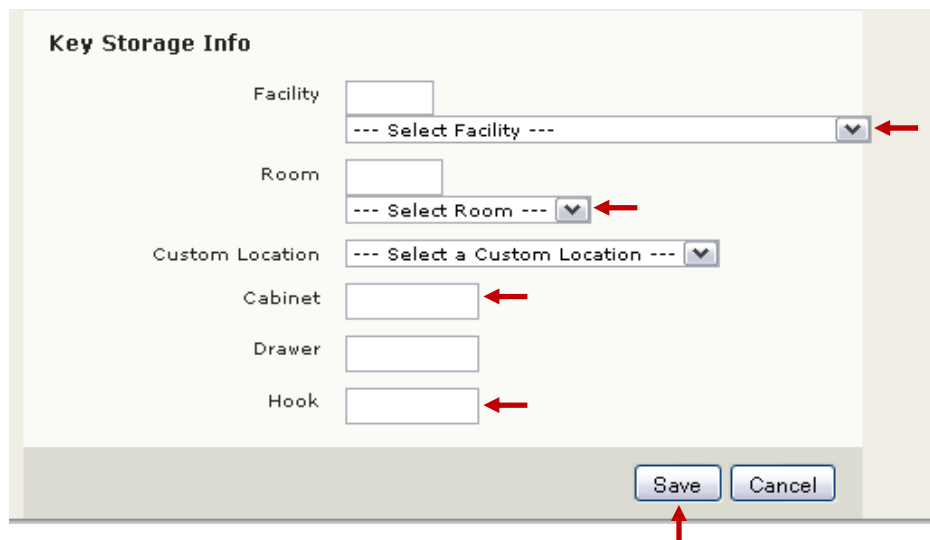
Key Assignment Info

Assign to [   ] Find User

Due Date [   ]

Assignee is a Responsible [ ]
Party?

- **Click "**Save" at the bottom of the page.

Note: If you are going to issue a newly cut key, it is highly recommended that you first place the key in storage and then assign the key. The system remembers the last storage location of an assigned key which is returned to storage, thus creating a storage location prior to issuance will save you a step when it is returned.

➢ To place a new key instance in storage:
  In the section Key Storage Information:

Key Storage Info

Facility [   ]
[--- Select Facility --- ▼]

Room [   ]
[--- Select Room --- ▼]

Custom Location [--- Select a Custom Location --- ▼]

Cabinet [   ]

Drawer [   ]

Hook [   ]

[Save] [Cancel]

- **Choose** the facility by facility code or use the drop down menu
- **Choose** the room within the facility from the drop down options

or

- **Choose** a *Custom Location* from drop down options (Note: custom locations must be established before using this option. See
- Manage Custom Storage Locations on page 59 for more information.)
- **Identify** the cabinet **or** drawer **and** hook
- **Click** "Save".
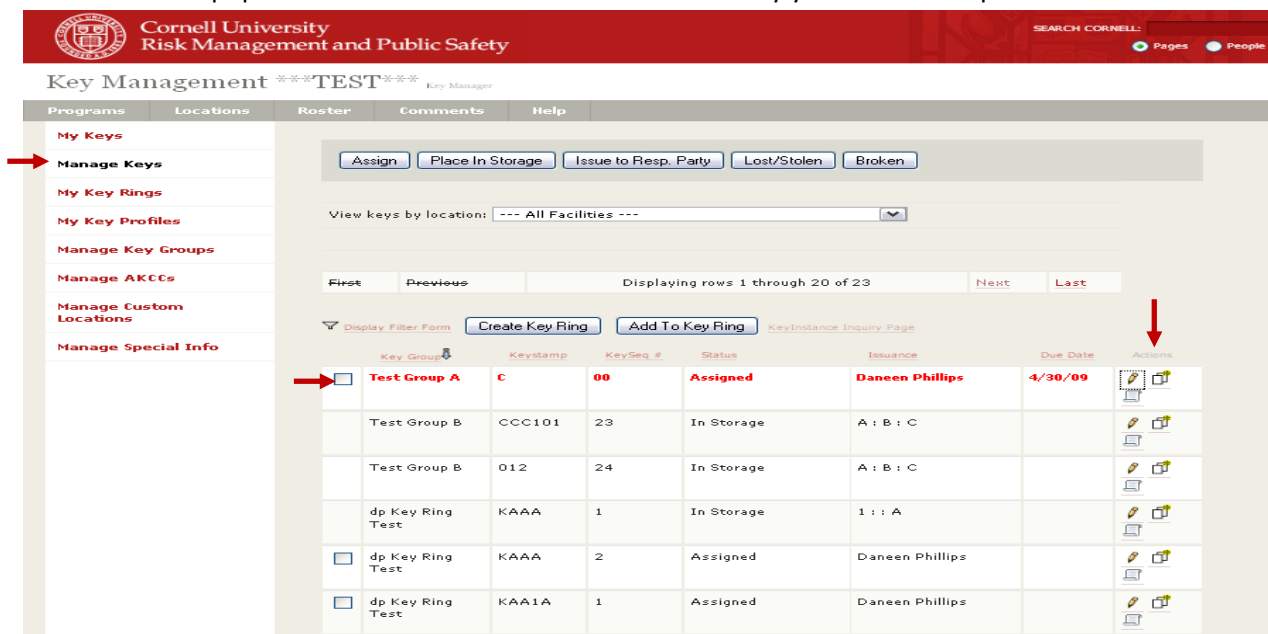
Note: If you are going to store a broken key until you send it to the Lock Shop, you will need to identify where the key is being stored. If you use a special storage location for broken keys you could create a Custom Location in

Manage Custom Storage Locations on page 59.

➢ To duplicate a key instance:

You can duplicate an existing key instance if you have multiple copies of the same key instance.

- **Go To** "Manage Keys".

- **Click** to duplicate the key. This will open the Key Instance Info window pre-populated with the same information as the key you chose to duplicate.

- **Update** the Key Sequence to reflect the new key. If you have more than one key with the same Key Sequence, the system will provide you with a warning that the key is a duplicate.

Note: Per Policy 8.4, keys must be uniquely marked to facilitate the tracking of individual key instances. Because duplicate keys currently exist on campus, the KMS allows this functionality. It is strongly suggested that, if possible, you update sequence numbers as you enter keys into the KMS and stamp the keys with the new sequence numbers.
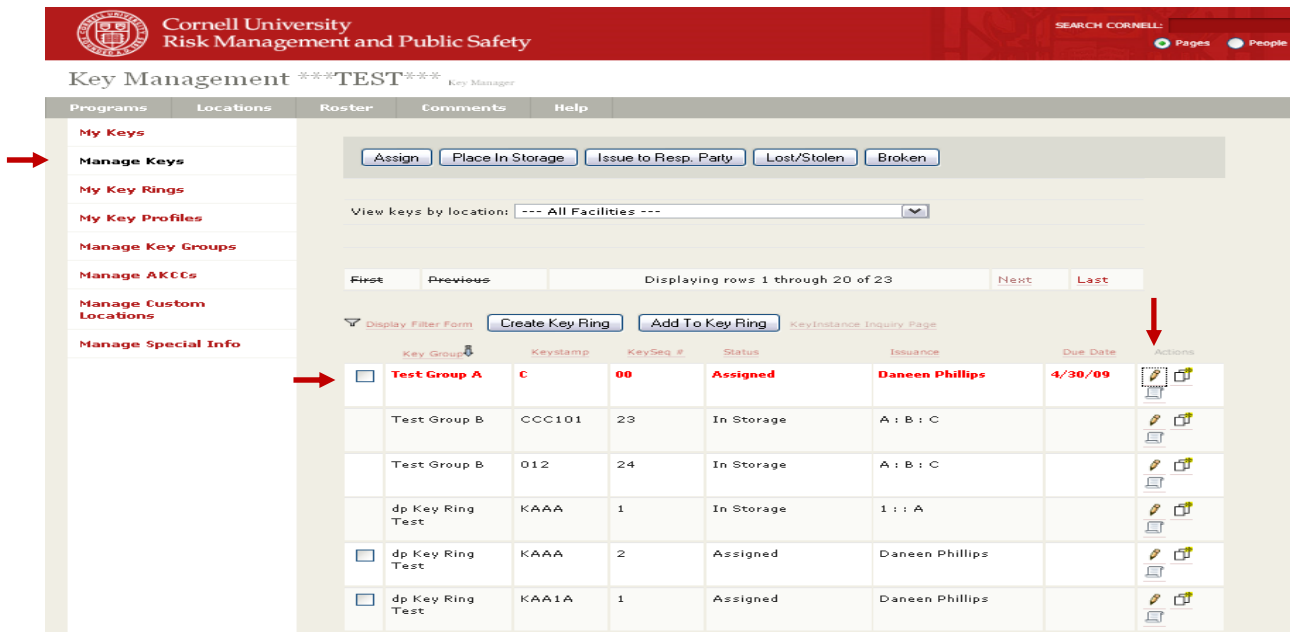
- **Complete** the Key Assignment Info or Key Storage Info as indicated above.

➢ To edit key instances:

You can edit key instance data during the creation process in order to correct data entry errors. (All edit changes will be tracked in the log.)

- **Go To** "Manage Keys".
- **Choose** the key; by clicking checkbox
- **Click** "Edit" icon

The following screen will open:

From this screen you can edit the following information: Key Sequence, Key Stamp, Key Group, Key Ring and/or add any notes.
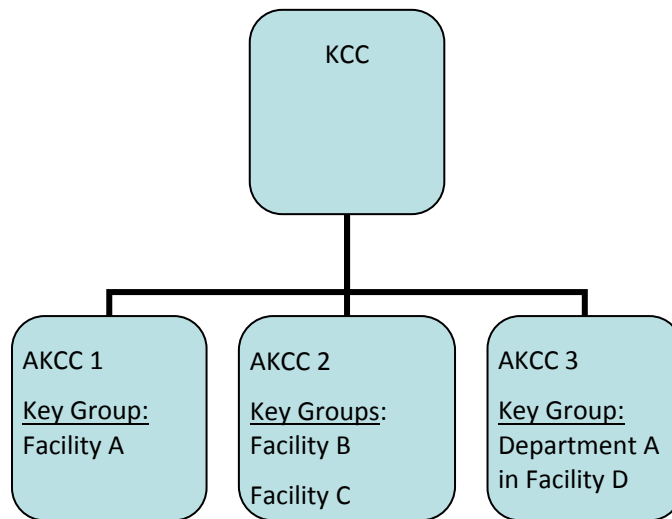
Edit the appropriate information.

- **Click** "Save".

Create Your Key Management Organizational Structure

Each KCC can have multiple Associate Key Control Coordinators (AKCCs) that manage groups of keys for the KCC. AKCCs may be organized by department or facility or any combination that makes sense for the unit. As you think about the most appropriate structure for your organization, please bear in mind: Each AKCC may manage more than one key group, and each key group can be managed by multiple AKCC; however, each key can be assigned to one and only one key group.

```
                    ┌─────────────┐
                    │     KCC     │
                    │             │
                    └──────┬──────┘
          ┌────────────────┼────────────────┐
    ┌──────────┐     ┌──────────┐     ┌──────────┐
    │ AKCC 1   │     │ AKCC 2   │     │ AKCC 3   │
    │          │     │          │     │          │
    │Key Group:│     │Key Groups:│    │Key Group:│
    │Facility A│     │Facility B│     │Department A│
    │          │     │          │     │in Facility D│
    │          │     │Facility C│     │          │
    └──────────┘     └──────────┘     └──────────┘
```

Manage AKCCs

- To add Associate Key Control Coordinators for your college/unit:
  (See definition for AKCC role)

  - **Go To "**Manage AKCCs".
  - If the AKCC has already been entered in the KMS, **choose** the AKCC from *Select from Dropdown.*
  - **Click "**Add New AKCC".

- To add a new AKCC to the KMS:
  - **Enter** the person's Netid
  - **Click "**Add New AKCC".

If you need assistance finding a user:

- **Select** the Find User field.
- ✓ **Enter** the appropriate information (last name, first name)
- ✓ **Click** "Find".

- **Click** "Select" on the right of the person's name
  This will add the person to the list of authorized AKCCs for your college/unit.

➢ To remove an AKCC as authorized for your college/unit:

- **Go To "Manage AKCCs".**

- **Click** "Delete" to the right of the person to be removed.
- **Click** "OK". Note that deleting an AKCC will remove that person from your key groups. If necessary, remember to assign a new AKCC(s) to those key groups.

Organize Your Keys

Once your profiles are established in the KMS with access locations and you've created your key management organizational structure, you should organize your keys in the KMS. KCCs organize keys into key groups. These groups may be by department or building or any grouping that makes sense to your organization.   You can assign a Key Group to one or more AKCC to manage. All AKCCs with permission to manage a Key Group will see all of the keys in that group. However, each key can be assigned to one and only one Key Group.

```
                        ┌─────────────────┐
                        │                 │
                        │       KCC       │
                        │                 │
                        └────────┬────────┘
            ┌────────────────────┼────────────────────┐
  ┌─────────┴─────────┐ ┌────────┴──────────┐ ┌────────┴─────────────┐
  │ AKCC1             │ │ AKCC2             │ │ AKCC3                │
  │                   │ │                   │ │                      │
  │ Key Group:        │ │ Key Groups:       │ │ Key Group:           │
  │ Facility A        │ │ Facility B        │ │ Department A in      │
  │                   │ │                   │ │ Facility D           │
  │ Facility B        │ │ Facility C        │ │                      │
  └───────────────────┘ └───────────────────┘ └──────────────────────┘
```
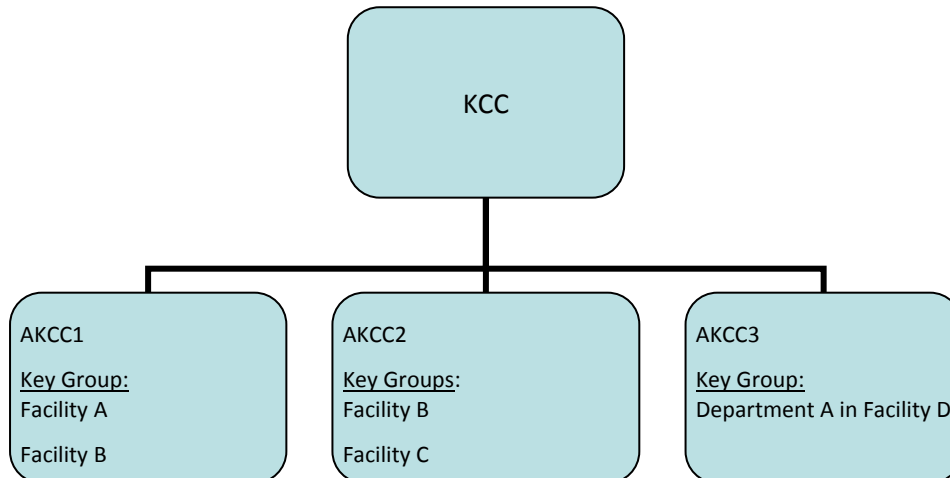
Note in the example above, both AKCC1 and AKCC2 can manage keys for Facility B because they have both been given access to that key group.

Manage Key Groups

➢ To view key groups:

- **Go To "**Manage Key Groups".

➢ To create a key group:

- **Go To** "Manage Key Groups".
- **Enter** the Group Name in text field.
- **Click** "Save".

➢ To rename a key group:

- **Go To** "Manage Key Groups".
- **Click** "Edit".

- **Edit** the key group name in the text box
- **Click** "Update".

➢ To authorize an AKCC for one or more key groups:

- **Go To** "Manage Key Groups".

- **Click** "Edit" next to the Key Group you wish to modify.

The following screen will open:

- From the list of Available AKCCs, **highlight** the name of the AKCC you wish to add to the group and **click** the right arrow to move name to Currently Assigned.

- **Click** "Update".

➢ To remove authorization for an AKCC for one or more key groups:

- **Go To** "Manage Key Groups".

- **Click** "Edit" next to the Key Group you wish to modify.

The following screen will open:

- From the list of Currently Assigned AKCCs, **highlight** the name of the person you wish to remove and **click** the left arrow to move name to Available

- **Click "**Update".

➢ <u>To remove a key groups:</u>

A key group cannot be deleted; however it can be renamed to be another key group. As part of this process, keys that shouldn't be part of the new key group should be reassigned.

- **Click** "Manage Keys" and reassign keys as appropriate. (See on Manage Keys on page 52.)

- **Filter** for the Key Group you are interested in removing.

- **Click** "Edit" and assign each key in the group to another key group

- **Click** "Manage Key Groups".

- **Click** "Edit" beside the key group you wish to remove.

- **Remove** all AKCCs from the currently assigned list for the key group.

- If appropriate, you can change the key group name either to something temporary, or to another key group you would like to use.

My Keys

This screen allows you to view keys, assign keys, place keys in storage, issue keys to a responsible party, or identify as lost/stolen or broken.

➢ To view keys within your unit:
Use this screen to view keys by facility.

- **Go To** "My Keys"
  To view a specific item in ascending / descending order; **Click the** item and an arrow will appear click again to reverse order

➢ **To view an activity log :**

- **Go To** "My Keys"
- **Click "**View Log" icon

This provides the complete transaction history for a specific key, see page display below.

➢ To filter the view:

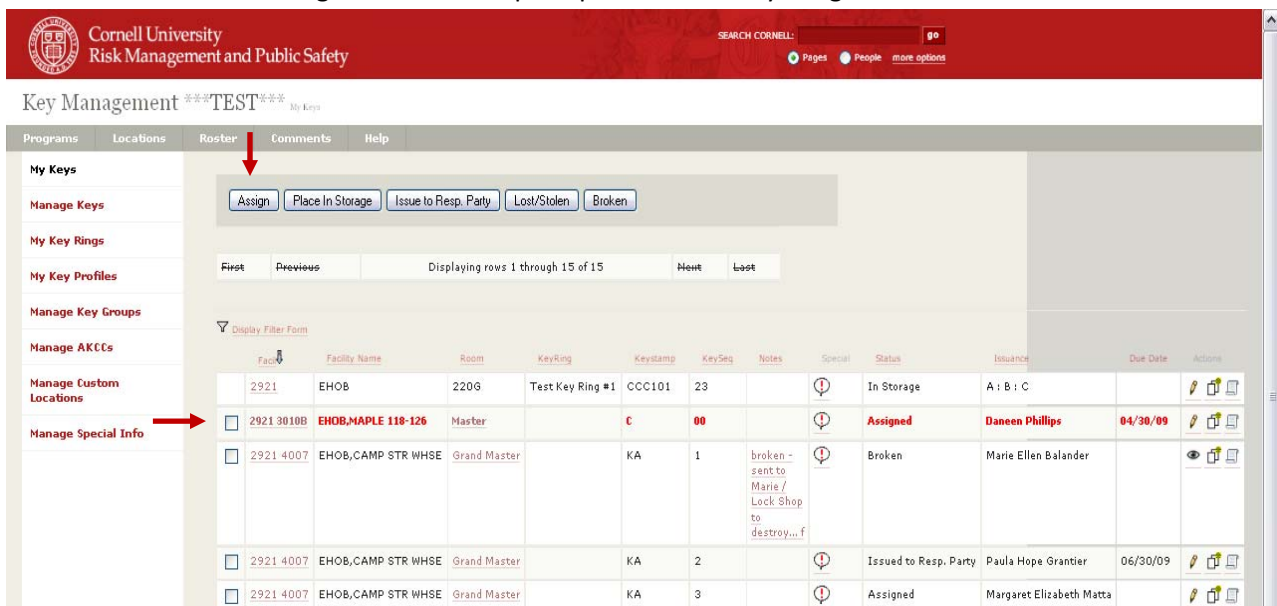- **Click** ▼ **to** display filter form. This will open drop down options which allow you to search by such things as: *facility, key ring, due date, etc.*
- **Click** on the item you wish to filter (this will highlight the item).
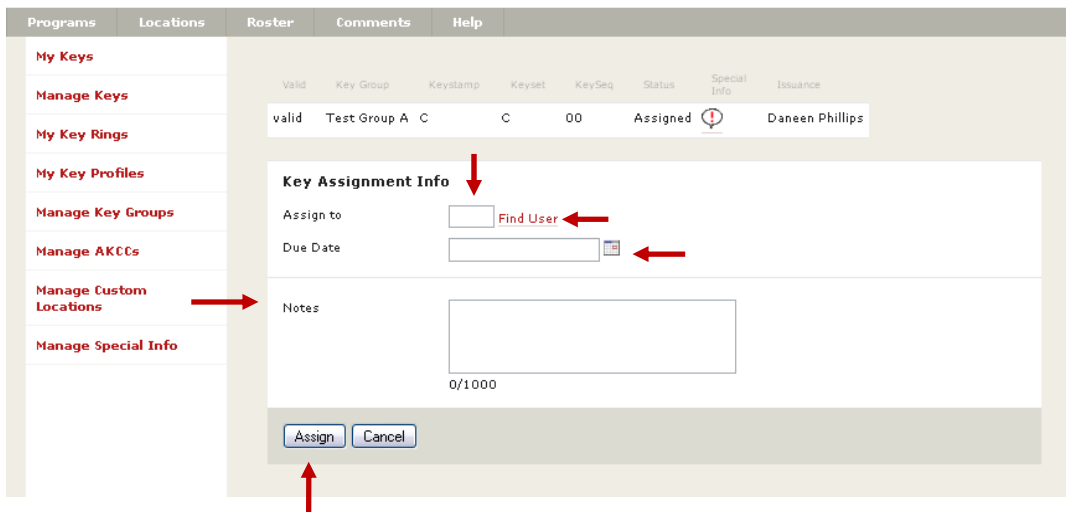- **Click** "Filter".

➢ To assign a key to a key holder:

- **Go To** "My Keys"
- **Choose** the key to assign by clicking in the checkbox on the left.
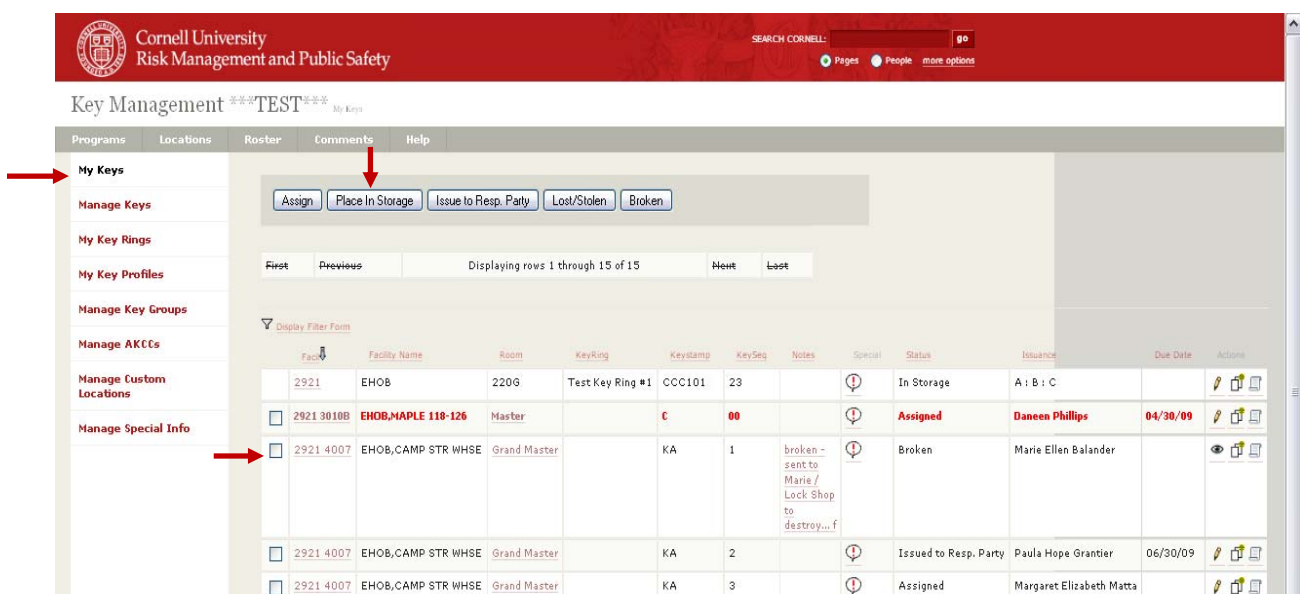- **Click "**Assign". You will be prompted to fill in key assignment information.

- **Enter** the Net ID or use the Find User option
- **Enter** the Due date. You would use this to assign the date that the key must be returned or audited.
  - o **Click** [calendar icon] to display calendar, select date
- **Notes:** briefly describe the purpose for the key being assigned
- **Click** "Assign".

➢ To place a key in storage:

- **Go To** "My Keys"
- **Choose** the key to place in storage by clicking in the checkbox on the left.
- **Click "**Place in Storage".

- **Choose** the *Facility* by entering the facility code or using the drop down options

- **Choose** the room within the facility

or

- **Choose a** *Custom Location* from drop down option. (Note: custom locations must already exist. See

- Manage Custom Storage Locations on page 59.)

- **Identify** the cabinet *or* drawer **and** hook

- **Notes:** make notes as needed, providing information regarding the key storage

- **Click** "Place In Storage".

➢ <u>To issue a key to a responsible party</u> (See Definitions)

- **Go To** "My Keys".
- **Choose** the key you wish to assign; by clicking in the checkbox
- **Click "**Issue to Resp. Party" (at the top or bottom of the page).

- **Enter** the Net ID or use the <u>Find User</u> option
- **Due date:** You would use this to assign the date that the key must be returned or audited.
  - **Click** [calendar icon] to display calendar, select date
- **Notes:** add to indicate the reason this key is being assigned (e.g.; visiting professor)
- **Click "**Issue to Resp. Party".

➢ To record a lost / stolen key:

If a key has been lost/stolen, per Policy 8.4, the key holder must **immediately** report the loss to their immediate supervisor. The supervisor should report the lost key to the KCC and the Cornell Police. The KCC is responsible to track within the KMS.

- **Go To** "My Keys".
- **Choose** the key you wish to mark as lost/stolen; by clicking in the checkbox
- **Click** "Lost/Stolen".

- **Notes** briefly describe circumstances of the loss of keys
- **Click** "Lost/Stolen".
- ✓ **If a replacement key** *is needed*, the request **must** be made to the KCC at the time of the report of the lost/stolen key. The KCC will request a new key using the University Key Order Form.

> To record a recovered lost/stolen key:
  (*The KCC must notify CUP that the key has been recovered*)
- **Go To "**My Keys".
- **Choose** the key you have recovered by clicking in the checkbox
  - ✓ *note: the key must be placed in storage, prior to re-assigning to a key holder*
- **Click "**Place in Storage".

- **Choose** *Facility* (enter the facility code or choose from the drop down options)
- **Choose** the room within the facility

or

- **Choose a** *Custom Location* from drop down option
- **Identify** cabinet *or* drawer **and** hook
- **Note:** add as needed, provide any information regarding the storage of this key
- **Click** "Place In Storage".

➢ To record a broken key:
   (The broken key or pieces __must__ be sent back to lock shop to be destroyed.)

   • **Go To "**My Keys".
   • **Choose** the key that has been broken by clicking in the checkbox next to key
   • **Click** "Broken".

   • **Choose** the Lock Smith at the Lock Shop you use in the Key Assignment Info
   • **Note:** briefly describe broken key was sent to the Lock Shop to be destroyed.
   • **Click** "Broken".

Manage Keys

This page allows the user manage keys by key groups, key stamp and sequence number, key holder or storage location, and due dates. From the Manage Keys page you can:

- Assign keys
- Place keys in storage
- Issue keys to a responsible party
- Identify keys as lost/stolen or broken
- Create key rings
- Add keys to key rings

➤ To view keys
    Use this field to organize assigned keys by key groups, key holders and the annual review of key holders and key groups.

- **Go To** "Manage Keys".
- To sort the keys in ascending or descending order, **click** the header and an arrow will appear [image] click again to reverse order [image]

➢ To filter the view:

- **Click** to display the filter form. This will open drop down options which allow you to search by the following: *key group, key attributes, key holders, and due dates.*
- **Click** on the item you wish to filter *(the information will be highlighted).*
- **Click** "Filter".

➢ To view instances made by Emergency & Service Personnel:

By Policy 8.4 – Management of Keys and Other Access Control Systems, Emergency and Service personnel may make instances of keys for entering a facility for emergency or service purposes. Within the KMS, Emergency and Service personnel may make instances of any keys whose profiles are not marked as "Secure." See the section " To view information about a secure key profile" on page 22.

- **Go To "**Manage Keys".
- **Click on** "Key Instance Inquiry Page" to view instances made by Emergency or Services personnel.

The following screen will be displayed showing all key instances made by Emergency or Services personnel.

➢ To create a key ring:

IMPORTANT: Key Rings must be created in the KMS before assigning the keys to individuals. They must be created with keys in storage.

- **Go To "**Manage Keys".
- **Choose** the keys that will be part of the key ring by clicking in the checkboxes
  The addition of keys to a key ring has the following constraints:
  - ✓ Keys **must** all be from the **same Key Group**
  - ✓ Keys must **not** already be **on another Key Ring.** *Note that keys that are already part of another key ring will not have a checkbox next to them.*
  - ✓ Keys **must be in storage**, *(i.e.,* **not** *assigned to an individual)*
- **Click "**Create Key Ring".

- **Input** Key Ring Description within the text field. The keys you've chosen to be in the key ring will be listed below.
- **Click "**Create Key Ring".

➢ To add keys to a key ring:

- **Choose** key(s) you wish to add to a key ring by clicking in the checkbox
  The addition of keys to a key ring has the following constraints:
    - ✓ Keys **must** all be from the **same Key Group**
    - ✓ Keys must **not** already be **on another Key Ring**. Note that keys that are already part of another key ring will not have a checkbox next to them.
    - ✓ Keys **must be in storage**, (i.e., **not** assigned to an individual)
- **Click "**Add To Key Ring".

First	Previous	Displaying rows 1 through 13 of 13		Next	Last

▽ Display Filter Form   Create Key Ring   Add To Key Ring   KeyInstance Inquiry Page

	Key Group ⇕	Keystamp	KeySeq #	Status	Issuance	Due Date	Actions
☐	Group 1	ABCD	2	Assigned	Eric W Bourdon		✎ ⬚ 📜
	Vehicle 402	SM	6	In Storage	W : : 12		✎ ⬚ 📜
☑	Vehicle 402	SM	5	In Storage	W : : 12		✎ ⬚ 📜
☐	aab	012	45	Broken	CRIME PREV : : 16		👁 ⬚ 📜
☐	aab	SM	2	Lost Stolen	: 13 : NA		👁 ⬚ 📜
☐	aab	SM	3	Destroyed	: 13 : 2		👁 ⬚ 📜
☐	aab	ORPH	00	In Storage	A : C : B		✎ ⬚ 📜

- **Select** the appropriate Key Ring from drop down. The keys you have chosen to add to the ring will be listed below.
- **Click** "Add Keys to Key Ring".

Key Ring Description	--- Select a Key Ring --- ▼
Key Group	Vehicle 402

Keys To be Added
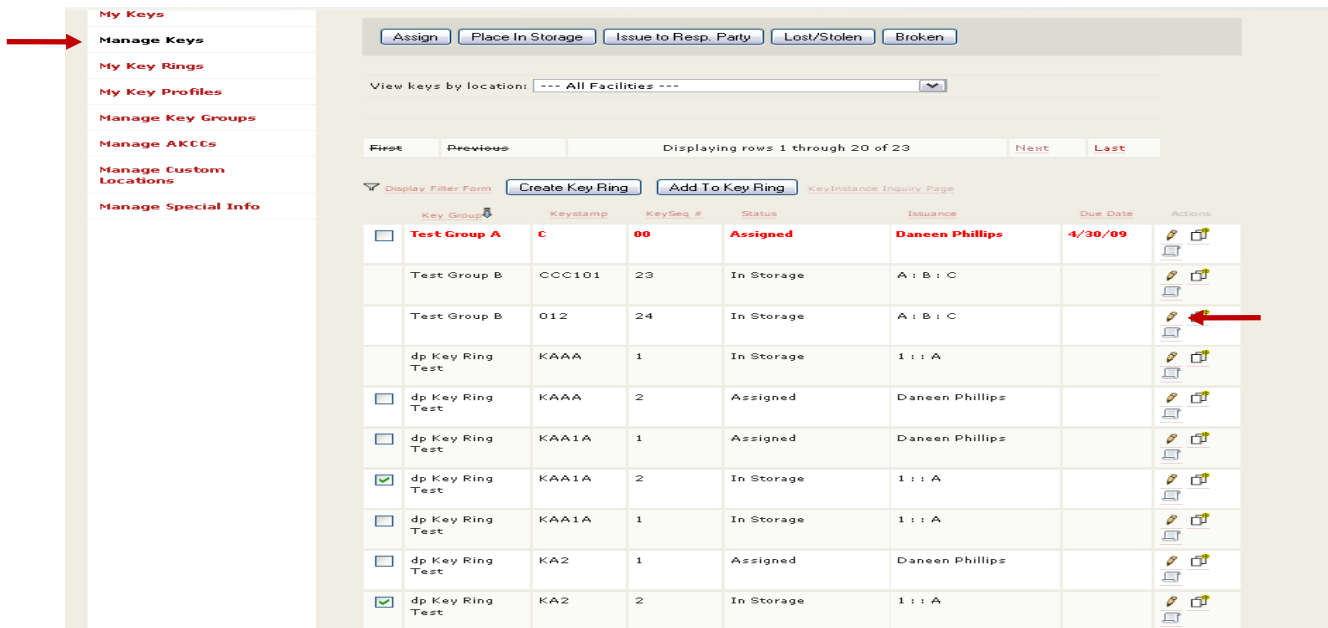
Keystamp	Keyset	KeySeq	Status	Special Info	Issuance
SM	SM	5	In Storage		W : : 12

Add Keys to Key Ring   Cancel

See the next section, My Key Rings, for information on managing additional attributes for key rings.

➢ To move a key to a different key group:
- **Go To** "Manage Keys".
- **Click** "Edit" icon

- **Select** the Key Group from the drop down box
- **Click** "Save".

My Key Rings

After a key ring has been created (see the steps in Manage Keys) you can assign the key ring to a key holder, place it in storage, issue it to a responsible party, or mark it as lost/stolen or broken. The procedures for a KCC are the same as those for an AKCC. See the section "My Key Rings" on page 77 in the **Associate Key Control Coordinator (AKCC) Procedures** section.

Manage Custom Storage Locations

➢ To create a Custom Storage Location:

- **Go To** "Manage Custom Locations".
- **Click** "Create New Custom Location".

- **Provide** a description of the custom location in text field.
- **Select** Facility Code from drop down – this building can be where the custom location is, or the building most associated with this custom location.
- **Select** Type from drop down list (vehicle, other)
- **Click** "Save".

Manage Special Information

This function will allow you to manage information about a location that would require approval by a specific individual prior to a key instance being assigned.   Such areas might include restricted access areas such as spaces with confidential information, hazardous materials, or hazardous conditions. This is a place to identify who the approver is and what special instructions need to be followed. For example, certain paperwork that needs to be completed, training that needs to be completed, etc. before providing access to the location.

➢ To create special information about a location:

- **Go To** "Manage Special Information".

- **Choose** Facility and room from the drop down options.

- **Push** the Tab button on your keyboard - this will open a field to add a user Net ID and any special instructions.

- **Click** "Create New".

When a space has been identified with special information, on the My Keys screen, this will be indicated with the following icon: ⊕ . When you take any actions with the key (such as assign the key or put it in storage), you will again see the icon indicating this location has special information associated with it.

To review the special information, click on the icon. ⊕

Reports

Currently reports are available for individual key transactions. These will allow you to print a summary of all of the keys that have been issued to an individual by you as the KCC or those issued by your AKCCs. In the near future, additional reports will be available to facilitate the annual review of key inventories. For additional details on reports, see "Reports" on page 89 in the AKCC Procedures Section. As a KCC you follow the same procedures as an AKCC in creating and printing reports.

Associate Key Control Coordinator (AKCC) Procedures

As AKCC you are responsible to:

- Receive and act on requests for keys, and changes to access.

- Store, protect, and distribute keys properly.

- Maintain a key record system.

- Issue temporary keys.

- Uniquely identify and mark keys.

- Conduct a review of keys and associated locations as requested by the KCC.

Note: Any of the responsibilities listed above, as well as the actions that an AKCC can perform within the KMS, can also be performed by a KCC.

Figure 5 – AKCC Responsibilities within the KMS

Lock Shop
1. Create key profiles

KCC
2. Assign access locations to key profiles
3. Assign AKCCs
4. Create key groups
5. Create key instances

AKCC
6. Create key rings
7. Assign keys and key rings
8. Sign keys and rings back in
9. Identify keys as lost/stolen or broken
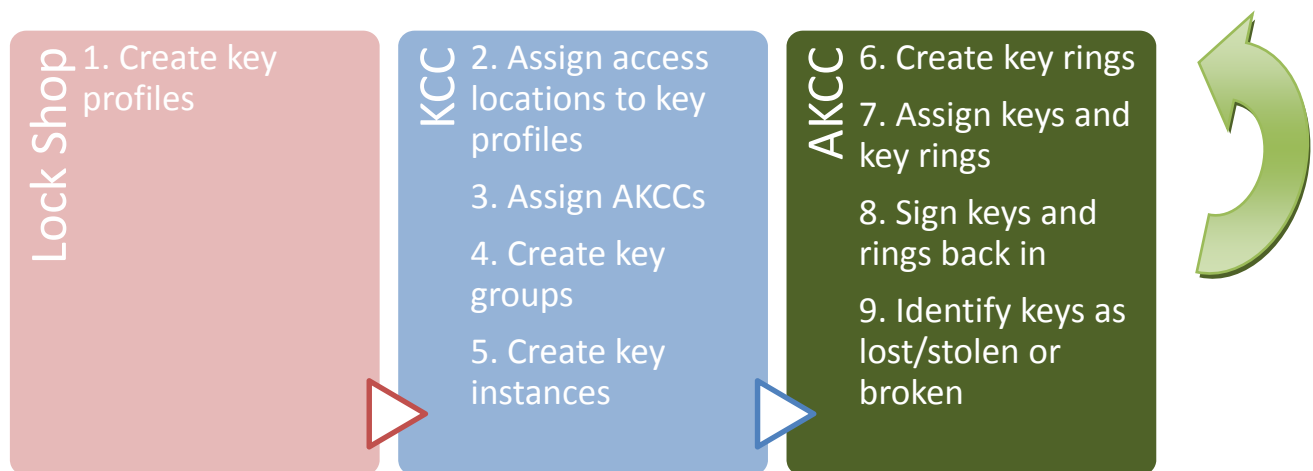
My Keys

This screen displays a list of all the keys that you as the AKCC are responsible to manage. These keys have been assigned to you by a KCC in key groups. (See "To authorize an AKCC for one or more key groups:
 on page 40.)

This screen allows you to view keys, assign keys, place keys in storage, issue keys to a responsible party, or identify as lost/stolen or broken.

> To view keys within your unit:
> *Use this screen to view keys by facility.*

- **Go To** "My Keys"
- To view a specific item in ascending / descending order; **Click the** item and an arrow will appear [icon] click again to reverse order [icon].

➤ To view an activity log:

- **Go To** "My Keys"
- **Click** the View Log icon .

This provides the complete transaction history for a specific key, see page display below.

➢ To filter the view:

- **Go To** "My Keys"
- **Click** ▼ to display the filter form, this will open drop down options which allow you to search by the following: *facility, key ring, due date, etc.*

- **Click** *(highlight)* on the item you wish to filter
- **Click** Filter

➤ To assign a key to a key holder:

- **Go To** "My Keys"
- **Choose** the key to assign; by clicking in the checkbox
- **Click "**Assign".

- **Enter** the Net ID or use the Find User option
- **Due date:** to assign a due date; select the date that the key must be returned or audited
- **Click** [calendar icon] to display calendar, select date
- **Notes,** briefly describe the purpose for the key being assigned
- **Click "**Assign".

➢ To place a key in storage:

- **Go To "**My Keys"
- **Choose** the key to place in storage; by clicking in the checkbox
- **Click "**Place in Storage". This works even when the key is already assigned.

- **Choose** *Facility*: enter the facility code or choose from the drop down options
- **Choose** the room within the facility

or

- **Choose a** *Custom Location* from drop down option
- **Identify** cabinet *or* drawer **and** hook
- **Note,** as needed, provide any information regarding the storage of this key
- **Click** "Place In Storage".

➢ <u>To issue a key to a responsible party:</u> (see definition)

- **Go To** "My Keys"
- **Choose** the key you wish to assign; by clicking in the checkbox
- **Click "**Issue to Resp. Party".

- **Enter** the Net ID or use the <u>Find User</u> option
- **Due date:** to assign a due date; select the date that the key must be returned or audited
- **Click** to display calendar, select date
- **Notes:** Indicate the reason this key is being assigned (e.g.; visiting professor)
- **Click "**Issue to Resp. Party".

➢ To record a lost / stolen key:

If a key has been lost/stolen, per Policy 8.4, the key holder must **immediately** report the loss to their immediate supervisor, the KCC and the Cornell Police. The KCC is responsible to track within the KMS.

- **Go To** "My Keys"
- **Choose** the key you wish to mark as lost/stolen; by clicking in the checkbox
- **Click "**Lost/Stolen".

Notes briefly describe circumstances of the loss of keys
- **Click** Lost/Stolen
    - ✓ **If a replacement key** is needed, the request **must** be made to the KCC at the time of the report of the lost/stolen key. The KCC will request using the appropriate form.

➢ To record a recovered lost / stolen key:
   (The KCC must notify *CUP that the key has been recovered.)*

- **Go To "**My Keys"
- **Choose** the key you have recovered; by clicking in the checkbox
- ✓ *note: the key must be placed in storage, prior to re-assigning to a key holder*
- **Click "**Place in Storage".

- **Choose** *Facility*: enter the facility code or choose from the drop down options
- **Choose** the room within the facility

or

- **Choose a** *Custom Location* from drop down option
- **Identify** cabinet *or* drawer **and** hook
- **Note,** as needed, provide any information regarding the storage of this key
- **Click** "Place In Storage".

➢ To record a broken key:

The broken key or pieces must be sent back to lock shop to be destroyed.

- **Go To "**My Keys"
- **Choose** the key that has been broken; by clicking in the checkbox
- **Click** "Broken".

- **Choose** Key Assignment Info *(the person at the Lock Shop)*
- **Note:** briefly describe broken key was sent to?? at the lock shop to be destroyed.
- **Click** "Broken".
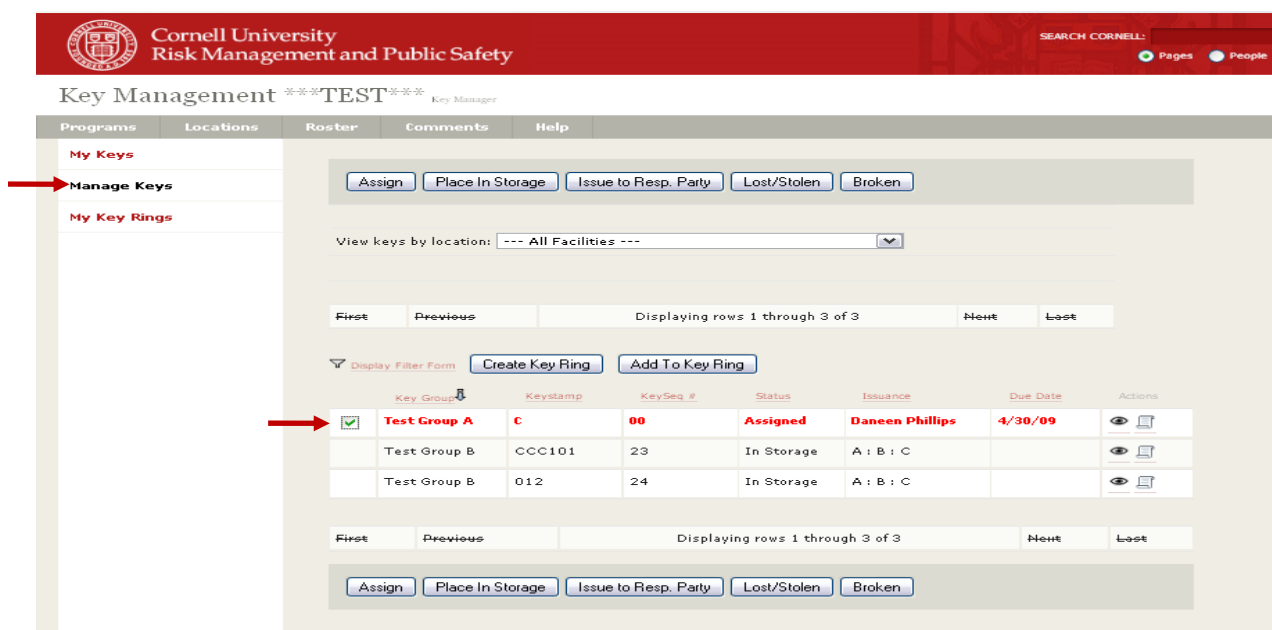
Manage Keys

This field allows the user to organize keys by groups, key holders, and manage due dates for specific college or unit.

➤ To view keys within your unit:
  Use this field to organize assigned keys by key groups, key holders and the audit of key holders and key groups.

  - **Go To "**Manage Keys"
    To view a specific item in ascending / descending order;

  - **Click the** item and an arrow will appear [icon] click again to reverse order [icon]

➢ To view an activity log:

- **Go To** "My Keys"

- **Click** the View Log icon ⬚.

This provides the complete transaction history for a specific key, see page display below.

➢ To filter the view:

- **Go To** "Manage Keys"
- **Click** ▼ **to** display the filter form, this will open drop down options which allow you to search by the following: *key group, key attributes, key holders, due dates.*

- **Click** *(highlight)* on the item you wish to filter
- **Click** "Filter".

➢ To create a key ring

IMPORTANT: Key Rings must be created in the KMS before being assigned keys.

- **Go To "**Manage Keys"
- **Choose** the keys to create a new key ring; by clicking in the checkbox
  The addition of keys to a key ring has the following constraints:
  ✓ *Keys **must** all be from the **same Key Group***
  ✓ *Keys must **not** already be **on another Key Ring***
  ✓ *Keys **must be in storage**, (i.e, **not** assigned to an individual)*
- **Click "***Create a Key Ring".*

- **Input** Key Ring Description within the text field
- **Click "**Create Key Ring".

➢ To add keys to a key ring:

- **Go To "**Manage Keys"
- **Choose** key(s) you wish to add to a key ring; by clicking in the checkbox
  The addition of keys to a key ring has the following constraints:
  - ✓ _Keys **must** all be from the **same Key Group**_
  - ✓ _Keys must **not** already be **on another Key Ring**_
  - ✓ _Keys **must be in storage**, (i.e, **not** assigned to an individual)_
- **Click "**Add To Key Ring".

- **Select** Key Ring from drop down
- **Click** "Add Keys to Key Ring".

My Key Rings

After a key ring has been created (see the steps above) you can assign the key ring to a key holder, place in storage, issue to a responsible party, or mark as lost/stolen or broken.

➢ To view key rings:

- **Go To** "My Key Rings"
  This provides a list all key rings that you as an AKCC are responsible to manage.

➢ To remove keys on key rings:

- **Go To** "My Key Rings"
- **Click the** Edit icon (on the right next to the appropriate key)

- **Click** the Remove from Key Ring icon ☒ (*next to the appropriate key you wish to remove*).

- **Click** "OK".

  This will prompt you to confirm the key storage location.

- **Edit** information, *if needed.*
- **Click "**Place in Storage".

➢ To assign a key ring:

- **Go To "**My Key Rings"
- **Choose** the Key Ring that you wish to assign by clicking in the checkbox
- **Click "**Assign"

- **Enter** the Net ID **or** use the Find User option
- Enter a due date if appropriate**.** You would use this to assign the date that the key ring must be returned.
- **Click** 🗓 to display calendar and select a date, or you can type a date into the box
- **Enter** notes if needed. You may choose to indicate the reason the key ring is being assigned or any other pertinent information.
- **Click** "Assign".

➢ To place the key ring in storage:

- **Go To "**My Key Rings"
- **Choose** the Key Ring to be placed in storage by clicking in the checkbox
- **Click** "Place in Storage".

- **Choose** the Facility by facility code or use the drop down menu- the last storage location is automatically entered
- **Choose** the room within the facility from the drop down options

or

- **Choose a** Custom Location from drop down options. (Note: custom locations have to already exist. See section
- Manage Custom Storage Locations on page 59.)
- **Identify** cabinet **or** drawer **and** hook.
- **Note** any information regarding the storage of this key or any other pertinent information
- **Click** "Place In Storage".

➤ To issue the key ring to a responsible party:

- **Go To "**My Key Rings"
- **Choose** the key ring you wish to assign by clicking in the checkbox
- **Click "**Issue to Resp. Party".

- **Enter** the Net ID or use the "Find User" option
- **Due date:** You would use this to assign the date that the key must be returned or audited.
- **Click** [calendar icon] to display calendar, select date- or you can type a date into the box mm/dd/yyyy
- **Note** any information regarding the reason this key ring is being assigned (e.g.; visiting professor) or any other pertinent information
- **Click "**Issue to Resp. Party".

➢ To record the key ring as lost/stolen:

If a Key Ring has been lost/stolen, per Policy 8.4, the key holder must *immediately* report the loss to their supervisor. The supervisor should contact the KCC who will report the loss to the Cornell Police as appropriate. The KCC is responsible to track the lost/stolen key within the KMS.

- **Go To** "My Key Rings"
- **Choose** the key ring you wish to mark as lost/stolen; by clicking in the checkbox
- **Click "**Lost/Stolen".

- **Note** a brief description of the circumstances regarding the lost/stolen key ring.
- **Click** "Lost/Stolen".
- ✓ *If a replacement key is needed*, the request **must** be made to the KCC at the time of the report of the lost/stolen key. The KCC will request the new key by completing the University Key Order Form.

➢ To record a recovered lost / stolen key ring:
    (Notify CUP that the key has been recovered.)

- **Go To "**My Key Rings"
- **Choose** key ring that has been recovered by clicking in the checkbox
- **Click "**Place in Storage" *(Note: the key must be placed in storage, prior to re-assigning to a key holder or responsible party)*

- **Choose** the Facility by facility code or use the drop down menu. The last known storage location will automatically be entered. You may edit the location or if it is appropriate click "Place In Storage".
- **Choose** the room within the facility from the drop down options

or

- **Choose a** Custom Location from drop down options
- **Identify** cabinet **or** drawer **and** hook
- **Note** any information regarding the key ring
- **Click** "Place In Storage".

➢ To record a key ring as broken:

- **Go To "**My Key Rings".
- **Choose** the key ring you wish to mark as broken by clicking in the checkbox. Note that this will "break" all keys on the key ring. If you wish to indicate only one key as broken, see the next section to record one key on a key ring as broken.
- **Click** "Broken". This will remove all keys from the key ring. They will be listed individually in Manage Keys and each will have a status of "Broken". There will be no keys associated with this key ring.

- **Choose** Key Assignment Info *(person at lock shop to "assign to")*

or

- **Choose** the *Facility* by facility code or using the drop down menu, which would be used if key(s) is being stored in your office before being sent to lock shop to destroy
- **Choose** the room within the facility from the drop down options

or

- **Choose a** *Custom Location* from drop down options (Note: custom locations have to already exist. See section
- Manage Custom Storage Locations on page 59.)
- **Identify** cabinet **or** drawer **and** hook
- **Note** briefly describe where broken key ring has been stored until sent to Lock Shop to be destroyed or other pertinent notes.
- **Click** "Broken".

➢ To record a key on key ring as broken:

- **Go To** "My Key Rings"
- **Choose** the key ring (where the key is that has been broken) by clicking the checkbox
- **Click** Edit icon

- **Click** to remove key from key ring

This will take you to the Place in Storage screen.

- **Click "**OK".

The page at https://cft-rmps.coldfusion.cornell.edu says:

Are you sure you want to remove this key from the ring? After you click OK, you will have to tell what the storage location of the key is.

OK   Cancel

This will take you to the "Place in Storage" screen.

- **Choose** the *Facility* by facility code or using the drop down menu, which would be used if key(s) is being stored in your office before being sent to lock shop to destroy

- **Choose** the room within the facility from the drop down options

or

- **Choose a** *Custom Location* from drop down options (Note: custom locations have to already exist. See section

- Manage Custom Storage Locations on page 59.)

- **Identify** cabinet **or** drawer **and** hook
- **Note** any pertinent notes.
- **Click** "Place in Storage".

 Now that the key has been removed from the ring, you will need to mark the key as broken. See "To record a broken key" on page 71.

Reports

Currently reports are available for individual key transactions. These will allow you to print a summary of all of the keys that have been issued to an individual by you as the AKCC. In the near future, additional reports will be available to facilitate the annual review of key inventories.

➢ To create an individual transaction log:

- **Go To** "Reports"
- **Choose** "Individual"
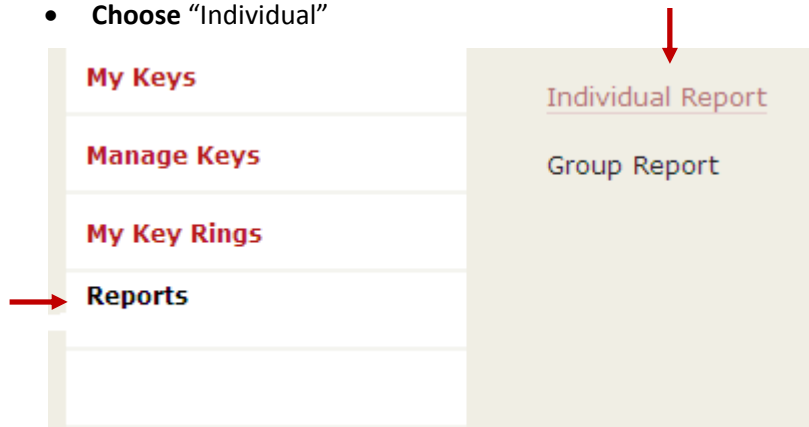
- **Enter the netid** of the person you would like a transaction log for
- **Click** "View Report"

The transaction log will display on the screen.

- **Choose** "Excel version of report" to get a report you can print and have the keyholder sign.

		My Keys
		Manage Keys
		My Key Rings
		Reports

Enter a NetID [   ] [View Report]

Excel version of report

KCC or AKCC Margaret Elizabeth Matta   Keys Issued To: Paula Hope Grantier

Netid: phg1

Phone Number: 607-254-1575

Cornell Affiliation: staff

Key Group	Key Set	Key Stamp	Sequence Number	Status	Date and Time Issued	Due Date	Access Room(s)	Access Building	Notes
dp test group	KA	KA	2	Issued to Resp. Party	03/13/2009 03:58 PM	06/30/2009	grandmaster		

A dialog box will appear indicating that you have chosen to open an excel file.

- **Choose** "Open with Microsoft Office Excel (default)"

Opening kms_report_dp338.xls

You have chosen to open

kms_report_dp338.xls

which is a: Microsoft Excel Worksheet
from: https://cft-rmps.coldfusion.cornell.edu

What should Firefox do with this file?

- ◉ Open with [Microsoft Office Excel (default) ▼]
- ○ Save File
- ☐ Do this automatically for files like this from now on.

[OK]   [Cancel]
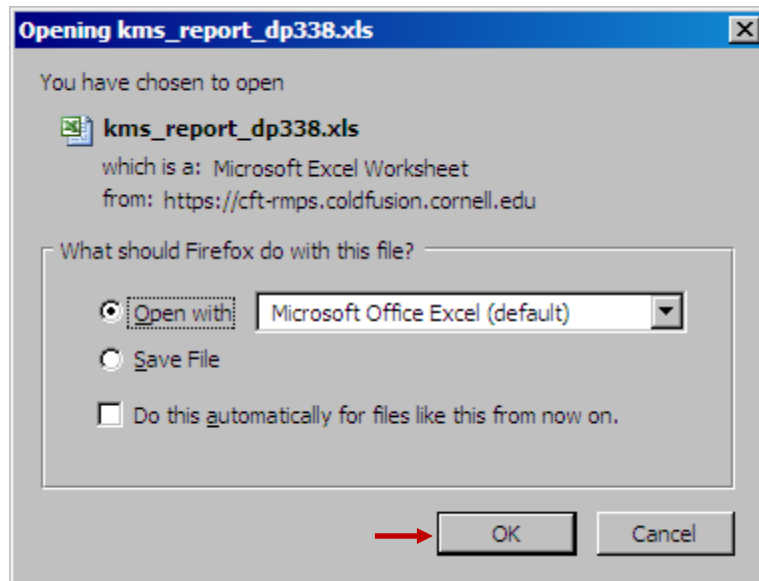
An additional dialog box will appear asking if you are sure the file is OK to open.

- **Choose** "Yes."

Microsoft Office Excel

⚠ The file you are trying to open, 'kms_report_dp338.xls', is in a different format than specified by the file extension. Verify that the file is not corrupted and is from a trusted source before opening the file. Do you want to open the file now?

[Yes]   [No]   [Help]
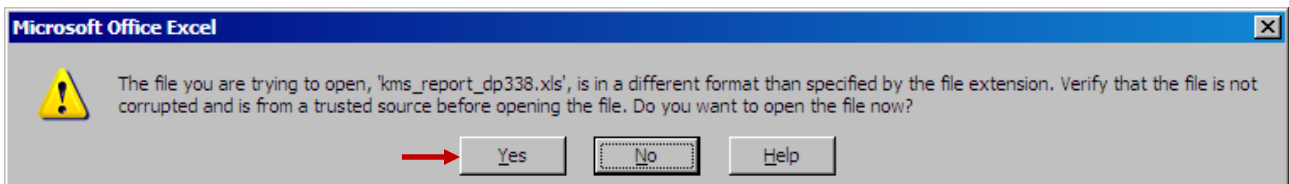
An Excel file will open with the transaction log for the keyholder.

Before printing this file, you'll want to make sure it will print on one page.

- From the Microsoft Menu in the top left , **choose** "Print", "Print Preview"

- **Choose** "Page Setup"
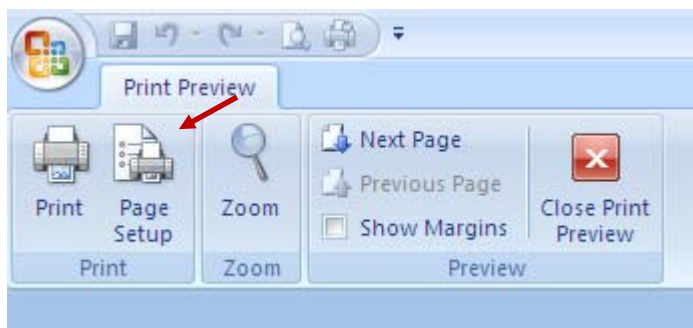
- **Choose** "Landscape" for the Orientation
- **Choose** "Fit to 1 page wide by 1 page tall" to fit the log on one page. You may need to choose 2 or more pages tall if the keyholder has a large number of keys.
- **Click** "OK"
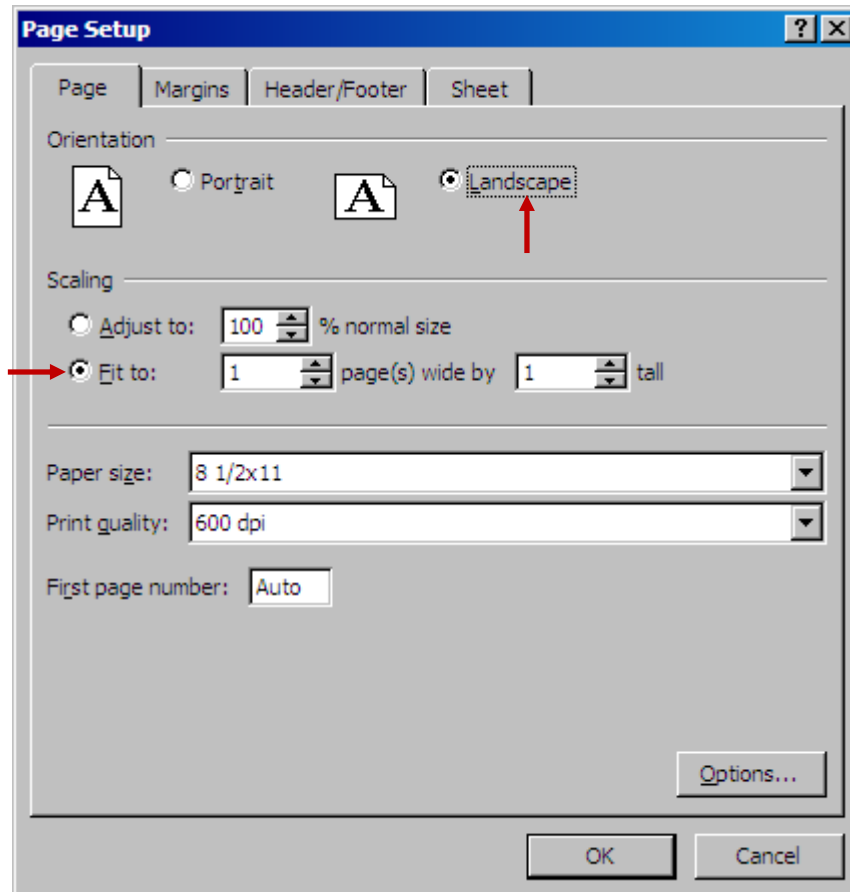
- **Have** the keyholder sign the transaction log
- **Sign** the transaction log yourself and file the log appropriately. This log will be used to capture the keyholder's signature when the keys are returned.

Appendix A – Forms

The following is a list of the forms available to help you manage access control:

FIRST, each unit and college must first authorize Key Control Coordinators (KCC) and Access Control Coordinators (ACC)

We are currently renewing authorizations for those that manage keys and access control devices for each college and unit. If you haven't completed this authorization since June 25, 2009 you will need to complete a new authorization.

Authorization of Access Control Coordinators and Key Control Coordinators is required by Deans and VPs. The authorization form should be completed, printed, signed and submitted to the Cornell University Police Crime Prevention Section in G-2, Barton Hall.

Designate to the Vice President or Dean This form may be used by the Dean or VP to designate an individual responsible to assign Access Control Coordinators and Key Control Coordinators. After this form is signed by the Dean or VP and submitted to Cornell Police, the designate would have the authority to sign the Authorization Form for ACCs and KCCs.

After authorization of KCCs and ACCs, the following forms may be used to order keys, track transactions and conduct annual reviews

University Key Order Form This form is used to order keys from the University Lock Shop. Specific instructions for completing and submitting a request for keys are included at the top of the form.

Transaction Log for Key Issuance and Annual Review This log can be used to record transactions associated with inventory tracking and issuance of keys. It can also be used for the review of key inventories that must be completed at least every two years. Best practice shows that done more frequently, annually or twice a year, the review is easier to keep current.

Appendix B – Frequently Asked Questions

1. **What was the driver for the policy changes?**

   This policy has been updated as a result of extensive examination of public safety and security practices and policies at Cornell and in support of a strategic priority launched to provide a higher level of safety and security for our community. This update provides enhanced policy guidelines for the management of physical keys and sets a campus-wide standard for card-access systems.

2. **I already inventory keys with my own system. Does this meet the policy requirements?**

   Your key inventory system must meet the following requirements from Policy 8.4:

   KCCs are required to maintain accurate documentation of all physical key transactions using a manual or automated system of record keeping. At a minimum, transaction records must contain the following information:

   - *Physical key assignment*
     - *Name of the device holder or storage location*
     - *Cornell affiliation of the device holder*
     - *Contact information for the device holder*
     - *Key set number and unique identifier of each key signed out*
     - *Due date for key, as appropriate*
     - *Date and time of sign-out*
     - *Date and time of sign-in*
     - *Signatory approval of the KCC or AKCC handling the transaction*
     - *Signatory approval of the recipient acknowledging that he or she alone will use this device as authorized*
   - *Change in physical key access location*
     - *Key system information (bitting number, keyway, etc.)*
     - *Location to be accessed*

3. **If my current tracking system meets the requirements of the policy, why should I use the KMS?**

   Per Policy 8.4 you must use the KMS for spaces with special access restrictions:

   All physical keys to spaces with special access restrictions (e.g., those with highly hazardous materials or highly valuable assets) must be inventoried in the university Key Management System (KMS).

   The KMS is a central inventory system. It allows the university to track physical keys in one location, rather than in a number of isolated locations across campus. This is important in the event of an emergency. Police and emergency response personnel will be able to use the system for reference and more quickly restore a situation to safety.

   Additionally, key inventories can be easily maintained and the KMS facilitates the review process of key inventories that must happen at least once every two years. The KMS ensures the key inventory requirements of Policy 8.4 are met. The KMS will also help units meet the requirement to review key inventories at least once every two years. If you do not use the KMS, your key inventory system is subject to auditing by the Cornell University Police.

   Because the KMS is used by the Lock Shops (both PDC and Campus Life), as well as Facilities Customer Service, Building Care and the emergency services personnel, processing of key requests will be easier via the KMS and tracking of keys becomes much more efficient with a common system between all of these organizations.

The cost to use the KMS is free and is therefore no more expensive than other current systems on campus. The KMS is maintained centrally and users are not charged a fee to use the system.

Phase II of the KMS project, expected to be complete during 2009, will include electronic routing of approvals. This means that keys may be requested and approved on-line – eliminating the need for routing paper forms within an organization to the KCC, then to the Cornell Police and on to the Lock Shop. This will considerable improve the efficiency of managing physical keys.

4. **I'd like to use the KMS. How do I get my existing key inventory information into the KMS?**

   A data conversion process is available for importing key inventory information into the KMS. See

   Appendix C – Importing Key Instance Information into the KMS.

5. **How long has the system been in place? Who is using it?**

   The KMS went into production in January 2009. It is currently being used by both Lock Shops (PDC and Campus Life), Facilities Customer Service, Building Care and the units that were involved in the development of the system, including: the College of Veterinary Medicine and the College of Human Ecology.

6. **Who was on the committee to develop the KMS?**

   The development committee for the KMS included a large number of stakeholders including: representatives of both Lock Shops (PDC and Campus Life), the Cornell University Police, Facilities Customer Service, Building Care, Campus Life administration, the College of Human Ecology and the College of Veterinary Medicine. CIT Information Services provided the business analysis, programming and database support.

   The stakeholders involved in the development of the system have a strong knowledge about keys and key systems. Their organizations are varied in the way they manage KCCs and AKCCs. The systems also range in size. The College of Veterinary Medicine has more than 10,000 key instances that are being managed within the KMS.

7. **How will you help me get started with the KMS?**

   Please review the slide presentation on-line at www.rmps.cornell.edu/keysinfo for a brief overview of the KMS and how it works.

   A key inventory conversion process is available to help you transition your existing data into the KMS. See

   Appendix C – Importing Key Instance Information into the KMS for more information.

   We will provide regular training classes on how to use the KMS. Please check the website (www.rmps.cornell.edu/keysinfo) for training class information.

8. **The policy says that all keys must be stamped with a unique identifier within 2 years. How do I accomplish this?**

We recommend stamping each key with a unique sequence number in addition to the key stamp or key set. (Reference

   Key Parts on page 13.) Risk Management & Public Safety has made available kits that may be borrowed to stamp your organization's keys. Contact the PDC Lock Shop at x5-7112 to request the next available stamping kit.

We recommend performing stamping on keys during the annual review of the KCC's key inventory. As each key in the inventory is verified it can be stamped. A best practice we've seen is to inventory and stamp the keys during an individual's annual performance dialogue.

In the interim until you get your keys uniquely identified with sequence numbers, the KMS will identify keys with duplicate sequence numbers when you go to issue the key. This will be a reminder that the key should be stamped with a unique sequence number before issuance.

9. **How is facility and people information kept current?**

The KMS ties to the facilities inventory and PeopleSoft, pulling both facility and people information into KMS and avoiding duplication of this information within the KMS. This ensures that the university's data of record is used for all transactions within the KMS.

10. **What if I need additional help or have questions about the KMS?**

First contact your KCC for help with the KMS. If your KCC is unable to address the question, send a request to kmsusers@cornell.edu.

Appendix C – Importing Key Instance Information into the KMS

As of the publishing of Version 1.0 of this manual, the key conversion process in just being finalized and is expected to be complete in August 2009. As soon as the final forms and process are available, this manual will be updated and posted on the following website: www.rmps.cornell.edu/keysinfo/kmsinfo.