CORNELL UNIVERSITY
POLICY LIBRARY

Management of Keys and Other Access Control Systems

POLICY 8.4

Volume: 8, Risk Management and Public Safety
Chapter: 4, Management of Keys and Other Access Control Systems
Responsible Executive: Executive Vice President and CFO
Responsible Office: Cornell University Police Department
Originally Issued: May 1999
Last Updated: April 13, 2018

POLICY STATEMENT

Cornell University 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.

REASON FOR POLICY

The university must maximize personal safety and protect property.

ENTITIES AFFECTED BY THIS POLICY

- All units of the university and anyone accessing Cornell-owned or –operated facilities.

◆ **Note**: Some facilities occupied by Cornell may not be covered by this policy.

WHO SHOULD READ THIS POLICY

- College, unit, and department administrators
- Deans, directors, and department heads
- Key control coordinators
- Access control coordinators
- Individuals, including faculty, staff, students, vendors, guests, and visitors, in possession of access devices

WEB SITE ADDRESS FOR THIS POLICY

- This policy: www.dfa.cornell.edu/policy/policies/management-keys-and-other-access-control-systems
- University Policy Office: www.policy.cornell.edu

Cornell Policy Library
Volume: 8, Risk Management and Public Safety
Responsible Executive: Executive Vice President and CFO
Responsible Office: Cornell University Police Department
Originally Issued: May 1999
Last Updated: April 13, 2018

POLICY 8.4

Management of Keys and Other Access Control Systems

CONTENTS

POLICY 8.4

Management of Keys and Other Access Control Systems

RELATED RESOURCES

University Policies, Documents
University Policy 3.22, Safekeeping of Financial Assets, Including Cash, Checks, and Securities
University Policy 4.6, Standards of Ethical Conduct
University Policy 5.9, Access to Information Technology Data and Monitoring Network Transmissions
Campus Code of Conduct
Campus Life Policy Library, “Keys, Cards, and Other Access Control Devices”
Cornell University Design and Construction Standard 16722
Cornell University Design and Construction Standard 08710
Unit policies and procedures

Forms and Tools
Access Card and Key Control Authorization Form
Key Management System
University Key Order Form
Event Registration Form
Veterinary Library Access Authorization Form

POLICY 8.4

Management of Keys and Other Access Control Systems

CONTACTS, ITHACA CAMPUS UNITS

The first point of contact for device holders and others with questions about this policy is the unit administrative office. The list of contacts below is provided for those with additional questions about specific issues.

Ithaca Campus Units

Subject	Contact	Telephone	E-mail/Web Address
Policy Interpretation and Clarification	Cornell University Police Department (CUPD)	(607) 255-4393	accesscontrol.cornell.edu/kms/
Access Card Replacement/Issue	University Registrar	(607) 255-4232	univreg@cornell.edu
Campus Card Access System	Cornell University Police Department (CUPD)	(607) 255-7874	accesscontrol@cornell.edu accesscontrol.cornell.edu/kms/
Changing and Maintaining Access Devices	Access Control Program	(607) 255-7874	accesscontrol@cornell.edu accesscontrol.cornell.edu/kms/
	Facilities and Campus Services Customer Service	(607) 255-5322	
	Campus Life Multi-Trade Shop	(607) 255-2074 (607) 255-6862	
Duplicating Physical Keys	Crime Prevention Unit of the Cornell University Police Department (CUPD)	(607) 255-7404	crime_prevention@cornell.edu
	University Lock Shop	(607) 255-4841	
	Campus Life Multi-Trade Shop	(607) 255-2074 (607) 255-6862	
Exceptions to Central Card Access System	Chief of the Cornell University Police Department (CUPD)	(607) 255-8945	
Key Management System	Cornell University Police Department (CUPD)		accesscontrol@cornell.edu accesscontrol.cornell.edu/kms/
Planning a Key System	University Lock Shop	(607) 255-7112	
	Campus Life Multi-Trade Shop	(607) 255-2074 (607) 255-6862	
Planning an Access Control System	Access Control Program	(607) 255-7874	accesscontrol@cornell.edu accesscontrol.cornell.edu/kms/
	Facilities and Campus Services, Electrical Engineering	(607) 255-1825	
	University Electric Shop	(607) 255-4746	
Security and Loss Prevention Surveys	Crime Prevention Unit of the Cornell University Police Department (CUPD)	(607) 255-7404	crime_prevention@cornell.edu

POLICY 8.4

Management of Keys and Other Access Control Systems

CONTACTS, WEILL CORNELL CAMPUS UNITS

The first point of contact for device holders and others with questions about this policy is the unit administrative office. The list of contacts below is provided for those with additional questions about specific issues.

Weill Cornell Campus Units

Subject	Contact	Telephone	E-mail/Web Address
Policy Interpretation and Clarification	Senior Director, Engineering and Maintenance	(212) 746-2950	ajryan@med.cornell.edu
Access Card Replacement and Access Problems	New York Presbyterian Hospital (NYPH) Security ID Card Unit	(212) 746-1837	
Campus Card Access System	New York Presbyterian Hospital (NYPH) Campus Card Access Administrator	(212) 746-1942	jcurti@nyp.org
Changing and Maintaining Access Devices	Engineering and Maintenance Dispatcher	(212) 746-2288	
New and Replacement Keys	Engineering and Maintenance Dispatcher	(212) 746-2288	
All Other Lock and Keying Issues	Supervisor, Carpentry and Finishes	(646) 962-3230	jcurti@nyp.org
All Other Card Access Issues	Financial Manager, Engineering and Maintenance	(212) 746-1089	gjbrend@med.cornell.edu

POLICY 8.4

Management of Keys and Other Access Control Systems

DEFINITIONS

These definitions apply to terms as they are used in this policy.

Access Card	A Cornell ID card issued by the university and assigned to a specific individual. OR A temporary access card issued or otherwise authorized by the university to access control coordinators (ACCs), to be used only when an ID card is not available.
Access Control Coordinator (ACC)	An individual responsible for assigning and maintaining access control for access cards.
Access Control System	Any mechanical or electronic device or devices used to secure a university space, building, room, closet, or vehicle. Door hardware includes, but is not limited to, card readers, biometric readers, combination locks, lock boxes, lock cylinders, automatic door operators, closers, and hinges.
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).
Campus Card Access Administrator	An individual responsible for maintaining the campus card access system. For Ithaca campus units, this is a senior programmer.
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).
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.
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 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).
Key Sequence	A sequence number assigned to a physical key that differentiates it from other keys of the same cut and key stamp.
Key Stamp	A series of letters and/or numbers stamped onto a physical key for purposes of identification.
Key Tag	An identification device with a unique number, usually attached to a key ring. Key tags are available from the Cornell University Police Department (CUPD) in G-2 Barton Hall.

POLICY 8.4

Management of Keys and Other Access Control Systems

DEFINITIONS, CONTINUED

Master Device	An access device, specifically for card access, used to open doors to a set of rooms, such as those on a particular floor, or those in an individual department, to which access is necessary by an individual. Only a unit head or designee is authorized to issue a master device.
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).
Responsible Party	A Cornell employee responsible for the access devices provided to a person who is not a Cornell student, faculty, or staff member.
Service Access	Access for the purposes of providing maintenance, repair, and building care services.
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.
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.

POLICY 8.4

Management of Keys and Other Access Control Systems

RESPONSIBILITIES – ITHACA CAMPUS UNITS

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	Provide planning assistance, design review support, or design service for new or upgraded access control systems. 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.

POLICY 8.4

Management of Keys and Other Access Control Systems

RESPONSIBILITIES -- ITHACA CAMPUS UNITS, continued

	Authorize ACCs and KCCs for the college or unit using the "Access Card and Key Control Authorization Form" (see "Related Documents, Forms, and Tools").
Device Holder	Maintain control of issued access devices. Prevent unauthorized use or duplication of access devices in their possession. Relinquish access devices when no longer authorized or needed. In the event of a lost access device, immediately notify your supervisor, and your ACC or KCC, or for students, the Campus Life Service Center.
Key Management System (KMS) Administrator	Maintain university KMS. Provide KMS system clarification and training to units. Notify users of outages. Administer KCC access rights.
Project Design and Construction, Design Section/Electric Shop	Provide planning assistance, design review support, or design service for new or upgraded access control systems.
Supervisor	Notify the ACC or KCC whenever there is a staffing change. Evaluate the need for access devices for new and existing personnel. Upon employee transfer or separation, recover access devices and return them to the ACC or KCC or AACC or AKCC.
University Electric Shop	Install, support, and maintain card access hardware. Provide estimates for new installations, upgrades, or conversions.
University Lock Shop	Store, protect, distribute, and maintain key system information (including bitting numbers, keyways, etc.) in the KMS. Reproduce keys as requested on "Key Order Forms" in accordance with this policy. Change locks as requested by individual units. Provide estimates for new installations, upgrades, or conversions.
University Registrar	Issue and replace access cards. Maintain a database of active and inactive cards.

POLICY 8.4

Management of Keys and Other Access Control Systems

RESPONSIBILITIES – WEILL CORNELL CAMPUS UNITS

Campus Card Access Administrator	Store, protect, and audit access devices/systems. Maintain a card access device record system. Maintain a campus central card access server and database. Administer access rights to the card access system.
Department Access Control Coordinator (ACC) and Key Control Coordinator (KCC)	Maintain records of access devices issued to department staff. Periodically review appropriateness of access. Upon separation of staff, return keys to the WCMC Locksmith. Return access cards to New York Presbyterian Hospital (NYPH) Security.
Department Head	Designate a person to be responsible for maintaining key and access control records (access control coordinator (ACC) and key control coordinator (KCC)) specific to the department and for authorizing access to the department's areas. Provide Security and Engineering and Maintenance with the name(s) of the department's ACCs and KCCs.
Device Holder	Maintain control of access devices. Return access devices when no longer authorized or needed for their business use.
Human Resources	Provide names of employees who are terminated to Engineering and Maintenance and NYPH Security.
New York Presbyterian Hospital (NYPH) Security	Periodically inspect access records. Issue new or replacement ID cards when authorized by Human Resources.
Supervisor	Upon separation or change in user access needs, retrieve all access devices and return them to the department's ACC and KCC.
WCMC Engineering and Maintenance	Arrange for the following services with the NYPH Locksmith, Weill Cornell Medical College (WCMC) Locksmith, or outside contractors as appropriate for the involved area: • Produce keys when appropriately authorized • Install/repair/replace access hardware

POLICY 8.4

Management of Keys and Other Access Control Systems

PRINCIPLES

Overview

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.

Purview of this Policy

Although access control systems may vary in different situations, this policy promulgates minimum standards that must be maintained throughout the university. This policy recognizes that certain agencies and units, by nature of their roles and responsibilities at the university, possess some access devices that allow for broad or unrestricted access. While this policy will not focus on the use of such access devices, it will address the tracking and control of such devices.

PRINCIPLES, continued

Considerations When Issuing Access to Spaces

Issuing access to particular individuals should be evaluated on a case-by-case basis. Below is a list of some factors to consider when making this determination. Units may have more stringent requirements.

- **Alternative Access**: Whenever possible, utilize alternative access methods (non-device-dependent), especially when the need for access is infrequent, arises because of a special circumstance, or is short-term. (In such circumstances, arrange for an individual responsible for a space to provide access, rather than issuing an access device).

Access devices should be issued only when necessary, especially when granting access to space that contains valuables, confidential materials, dangerous substances, or equipment.

- **Temporary Access**: When access is needed on a temporary, rather than permanent, basis, issue a temporary access device, and establish a clear time frame and procedure for return.
- **Hours of Work**: If a facility is unlocked during an individual's normal working hours, and access is not needed at other times, do not issue an access device.
- **Work Space**: Issue an access device that opens the least number of spaces as required for an individual to perform his or her job. This may range from access to a single space in one facility to multiple spaces within multiple facilities.
- **Card Access**: When possible, issue access via card access rather than issuing a key. Access provided via the card access system is easier to control and access is tracked via the central system.

Altering Locks and Card Access Systems

For reasons of personal safety, it is strictly prohibited for unauthorized individuals to alter access control systems in a way that excludes master key operation (or, in the card access system, emergency access level).

Sharing Keys/Access Devices

Sharing access devices is generally prohibited. In certain circumstances, when it is not practicable to have individual key assignments, and where access to a shared space is required by more than one person (e.g., a storeroom, a file cabinet), a site may be established for these purposes, at the discretion of the ACC or KCC, that is protected at a level of security as required by this policy (see the "Security and Audit Requirements" segment of this policy).

Cornell's Card Access System

All units using a card access system must use the central campus card access system, unless an exemption has been granted. As of the date of promulgation of this policy, any *new* stand-alone system must be specifically exempted from the central campus

POLICY 8.4

Management of Keys and Other Access Control Systems

PRINCIPLES, continued

card access system. In addition, any unit with an existing stand-alone system will have five years from the promulgation of this policy to convert to the central card access system or obtain an exemption. Approval for any exemption will be considered by the Director of Risk Management and Insurance, and will be based upon specific business needs, such as undue hardship

Emergency and Service Access

The ACC or KCC is responsible to ensure that emergency response and service personnel have proper access to facilities and spaces. These individuals are expected to abide by the principles of this policy and individual department/college/unit policy (which may be more restrictive).

Individuals who are temporarily without their access device(s) and locked out of spaces to which they have authorized access must follow their individual department/college/unit procedures to obtain access.

The Cornell University Police Department (CUPD) may provide access to authorized individuals who are temporarily without access to a particular space after consulting with a primary or secondary building coordinator, department manager, unit director, or college dean, or when emergency access, as defined in this policy, is required.

◆**Caution:** In the normal course of operations (i.e., except in emergency situations), custodians, Facilities Services staff members, Environmental Health and Safety personnel, and other individuals are prohibited from providing space access to individuals not in their departments, unless this task is part of their job responsibilities.

◆**Note:** In very rare circumstances, Facilities Services personnel are permitted to provide "forced" access to a secured space (e.g., breaking glass, entering through a window, cutting chains, removed cores, etc.), but only after consulting with the ACC, KCC, or the CUPD, or at the express direction of another emergency services provider, such as Environmental Health and Safety or a Fire Department official.

POLICY 8.4

Management of Keys and Other Access Control Systems

PROCEDURES, ITHACA CAMPUS UNITS

Access Control Coordinators and Key Control Coordinators

At the discretion of the college or division head, certain individuals will be designated as access control coordinators (ACCs) or key control coordinators (KCCs). At a minimum, ACCs and KCCs are responsible for the following:

- Handling requests for access devices, and changes to access
- Issuing temporary access devices
- Authorizing duplication of and distributing access devices, as appropriate
- Properly storing and securing access devices
- Uniquely identifying and marking access devices
- Maintaining access device records, including associated access locations
- Reporting lost keys to the Crime Prevention Unit of the Cornell University Police Department (CUPD), as appropriate
- Periodically initiating reevaluation of the need for access devices and retrieving them when necessary
- Conducting reviews of access devices/systems and associated locations at least every two years
- Designating associate ACCs (AACCs) or KCCs (AKCCs)

The college or division head must ensure that the Crime Prevention Unit of the CUPD has a current list of all ACCs and KCCs or designees. Updates to this list must be submitted, in writing, using the "Access Card and Key Control Authorization Form" (see "Related Documents, Forms, and Tools").

Requests for Keys, and Key or Lock Changes

Requests for duplication of keys used to secure buildings, rooms, or closets must be made through the Crime Prevention Unit of the CUPD by a KCC, using a "University Key Order Form" (see "Related Documents, Forms, and Tools"). The form must be complete and legible.

Other types of keys may be requested directly from the appropriate university lock shop using the "University Key Order Form", and do not require authorization by the CUPD (e.g., file cabinets, vehicles). Requests for any lock changes (e.g., core change, lock replacement, key system upgrade) must be made to the appropriate lock shop by the KCC, and must adhere to University Design and Construction Standards. To assist in these types of changes, the CUPD can conduct a security and loss prevention survey. Additionally, the lock shops can provide guidance for key system planning.

◆**Note**: Exemptions from these request procedures must be authorized in writing by the Crime Prevention Unit of the CUPD.

◆**Note**: Each key will be uniquely identified.

PROCEDURES, ITHACA CAMPUS UNITS, continued

Send the completed "University Key Order Form" to the Crime Prevention Unit of the CUPD, at cupkeys@cornell.edu, (or room G-2 Barton Hall), for approval. The original key to be duplicated should be sent to the appropriate lock shop, or the Campus Life Multi-Trade Shop. The approved "University Key Order Form" will be forwarded to the appropriate lock shop from the CUPD.

◆**Caution:** It is prohibited to make grand-mastering changes that restrict emergency access by the CUPD or other emergency service providers, or to install personal locks or deadbolts on university-owned or operated spaces. The CUPD and emergency service providers must be notified of any changes at the grand-master or emergency access level.

Master Keys

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.

◆**Caution:** Failure to report lost or stolen master keys may result in disciplinary action, up to and including termination of employment.

Requests for Card Access

The university has a campus-wide card access system. This system consists of an access control database that is centrally administered and locally managed, access control hardware that is installed in the individual buildings, and Cornell ID cards that are held by individual users. Typically, ID cards issued by the University Registrar's office are used as the access devices for the card access system.

All requests for repairs of card access hardware should be made through the Facilities Customer Service Center. If an exception to using the campus-wide card access system has been granted by the Director of Risk Management and Insurance, the exempted unit will not be required to follow this procedure.

Requests for new installations, conversions, or upgrades may be done through a Project Manager in conjunction with the campus card access administrator. Smaller projects can be requested via an estimate request through the Facilities Customer Service Center. Additionally, the Project Design and Construction, Design Section and Electric Shop can provide guidance for card access system planning.

All card access installations will meet the Cornell Design & Construction Standard 16722 Security and Access Control Systems.

It is prohibited to make changes to card access locations that prohibit emergency access by the CUPD or other emergency service providers.

POLICY 8.4

Management of Keys and Other Access Control Systems

PROCEDURES, ITHACA CAMPUS UNITS, continued

Lost or Stolen Access Devices

Students who lose residence hall room keys must immediately report the loss to the Campus Life Service Center. All other device holders must immediately report any lost, found, or stolen keys/access devices to their immediate supervisors, and ACCs and/or KCCs. The ACC or KCC should inform the CUPD as appropriate.

◆ **Note:** In the event of a lost key, the unit should assess the need to replace the cores of the locks at the associated locations. The CUPD can provide guidance in this determination. In the event of a lost access card, the ACC must ensure that access for this device is removed.

Physical Key Replacement

Any replacement keys needed due to loss, breakage, or theft will be made at the request of the KCC. Part of a broken key or a copy of the report of a lost or stolen key should be given to the KCC at the time of the request. Broken or outdated keys must be sent to the University Lock Shop, or, for Campus Life, the Campus Life Multi-Trade Shop, for disposal/destruction.

The handling of key deposits may be administratively burdensome, with the associated cash handling presenting an internal control risk. Units are encouraged to consider other mechanisms to ensure the return of keys. However, if required by individual departments, a deposit may be mandated for some keys. In such instances, the cash must be managed in accordance with University Policy 3.22, Accepting Cash and Checks, and placed in an account in Fund 420 (Current Fund, Liabilities Other), Function 104 (Deposits). Please contact your business service center for further assistance.

Access Card Replacement

All access cards will be replaced by the University Registrar's office except for Departmental Visitor Cards. Departmental visitor cards will be replaced by the local ACC.

Security and Review Requirements

Physical Keys

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

PROCEDURES, ITHACA CAMPUS UNITS, continued

- 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

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).

KCCs are expected to secure physical keys behind two locks (e.g., in a locked file cabinet inside a locked room). Likewise, all documents or systems containing physical key transaction information shall be kept secure and behind two locks.

All physical keys should also have a file key for use during duplication or key type verification.

Within two years of the issuance of this policy, all physical keys must be marked with a unique identifier (e.g., a key stamp and a sequence number). This mark may not be a room number or location. Key stamping kits are available to borrow from the University Lock Shop for these purposes.

◆ **Note**: It is recommended that all issued keys are associated with a key tag issued by the CUPD Crime Prevention Unit.

Card Access

ACCs are required to do the following:

- Maintain their segment information within the card access database
- Set expiration dates on access levels when required (e.g., temporary access for vendors or tradespeople)
- Regulate access to buildings with time zones and access levels
- Have a system in place to communicate access level changes to accommodate new hires, retirements, and separations.

POLICY 8.4

Management of Keys and Other Access Control Systems

PROCEDURES, ITHACA CAMPUS UNITS, continued

Both – Keys and Card Access

Unit heads are responsible to see that access device reviews are conducted with all device holders at least every two years.

KCCs are responsible for completing a documented physical key inventory review of all devices within their jurisdiction at least once every two years.

ACCs are responsible for the performance of a documented review of users and their access levels in the card access system within their jurisdiction at least once every two years.

Separation or Transfer

It is the responsibility of the immediate supervisor or human resources representative to collect all access devices issued to an individual at the time of transfer to a new department or separation from the university. This individual will then consult with the ACC and/or KCC to ensure that all devices are accounted for prior to transfer or separation. The ACC will remove any access in the card access system. Finally, the immediate supervisor or human resources representative must surrender all collected access devices to the ACC and/or KCC within 24 hours of collection, to enable proper and timely verification.

POLICY 8.4

Management of Keys and Other Access Control Systems

PROCEDURES, WEILL CORNELL CAMPUS UNITS

Key Requests

All key requests are to be approved by the appropriate Department Access Control Coordinator (ACC) and Key Control Coordinator (KCC) and submitted in writing to Weill Cornell Medical College (WCMC) Engineering and Maintenance. Keys will be cut by the New York Presbyterian Hospital (NYPH) Locksmith, the WCMC Locksmith, or a contracted locksmith as appropriate.

Requests for Card Access

Requests for card access must be made in writing from the ACC and KCC to the NYPH Campus Card Access Administrator.

Lost Keys or Access Cards

Lost keys or access cards must be reported immediately to NYPH Security. NYPH Security will arrange for lost access cards to be disabled.

Lockouts

Individuals that are temporarily without their appropriate access devices should contact NYPH Security for access to the work area. NYPH Security will verify the person's identity and the appropriateness of the requested access before providing access. All requests for lockout access will be logged, whether or not access was granted. Supervision within Security or Engineering and Maintenance can approve lockout access.

Lockout access to highly secured areas will not be provided without supervisory approval.

Installation/Repair/Replacement of Access Hardware

Requests for these services should be made to WCMC Engineering and Maintenance, who will arrange for the services to be performed by the NYPH Locksmith, WCMC Locksmith, or outside contractors as appropriate for the area involved.

Security and Review Requirements

Shared keys and access cards are to be signed in/out by the person responsible for the device.

Physical key inventories are to be secured appropriately by the person responsible for the items.

Separated Employees or Other Access Device Holders

The person's supervisor is responsible to retrieve all access devices and return them to the department's ACC and KCC.

POLICY 8.4

Management of Keys and Other Access Control Systems

INDEX

INDEX, continued