PRINCETON UNIVERSITY

Key Control Policy

Effective Date:	August 1, 2013	
Responsible Executive:	Mike McKay, Vice President, Facilities	
Responsible Office:	Facilities Department	
Contact:	Don Lowe, Facilities	(609) 258-4110
Last Update:	October 7, 2013	

I. POLICY STATEMENT

In the interest of providing the Princeton University community with a safe environment to learn, teach, live, and work, the University limits and controls keys to University facilities and spaces. Keys and locks to University facilities and spaces are the property of Princeton University, and should be obtained and managed in accordance with this policy. The specific purpose of this policy is to ensure that keys are issued only to appropriate persons and for appropriate reasons; to define the responsibilities of University key holders; and to provide for the responsible care of keys held by key holders. Keys are managed according to their risk category.

II. WHO is AFFECTED by this POLICY

This policy applies to all students, faculty, staff, vendors, designers, consultants, and contractors accessing University controlled areas. However, this policy does not include card access locks, keys for leased space, rental housing units, or construction sites wholly controlled by a contractor, as those are regulated by separate policies.

This policy shall be applied only when a lost key triggers a whole-building rekey, or where a building is being rekeyed as part of a normal rekey cycle. If a rekey is to accommodate a simple "in-kind" key replacement, the requirements of this policy are not triggered. However, if there are a high number of requests from a department for high- or medium-risk keys, the full requirements of this policy may also be triggered. Even though this policy may not be triggered in a given case, departments are encouraged to adhere to this policy, as it represents best practices for institutional key control.

III. DEFINITIONS

University Key – Key that opens University-controlled buildings, facilities, or structures, to include gates. For the purposes of this policy, this would normally exclude keys to lockers, desks, systems furniture, vehicles and equipment, or cabinets, all of which are controlled at the department level.

Exterior Door Key – Key that opens an exterior door to a building. On buildings controlled by card access this will be a high-security key. On buildings not controlled by card access this will be a standard key issued to building occupants.

High-Security Key – Key that opens locks that have a high-security core installed. Most of these locks are exterior doors where access is controlled by a card access system, although there are some interior doors with a high-security core.

Master Key – Key that opens all (or most) interior locks within a given building.

Sub-Master Key – Key that opens all locks within a department, or group of departments, or other defined area within a building.

Operator Key – Key that opens a few individual locks within a building. Typical configuration would be that an operator key opens the main door into a department, and one or more other doors within that department.

Restricted Access Key – Certain areas, although within a department's space, may have restricted access due to an increased need for security or because of a special hazard. Typical areas would include certain research and lab areas, special storage areas, electrical-mechanical spaces, high-voltage rooms, roof

access, exterior gates, athletic areas, or areas where hazardous items are contained therein, and where routine access is not appropriate.

Temporary Key – Temporary keys are keys signed out at the Lock Shop customer service window, and are for persons who have a legitimate access need, but who do not need such access on an ongoing/indefinite basis. Typical sign outs are maintenance employees needing short-term access to fulfill a work request, or a University construction project manager needing access on a long-term basis to complete a project.

Lock and Key Coordinator – Within each department the Lock Shop will coordinate new key requests, key transfers, and core changes with the department's office head, dean, or chairperson. If not performing the function themselves, department heads, deans, and chairpersons are responsible for assigning someone in their department to the function of Lock and Key Coordinator, and for notifying the Lock Shop when the designated person is no longer authorized to request keys/lock changes.

Key Risk Category – Key control is based upon the degree of risk created should a key become unaccounted for (lost/missing/stolen). Persons controlling a "high-risk" or "medium-risk" key are responsible to a larger degree than an "operator" key holder for the security of campus assets and the University community. Specific definitions are as follows:

a. Low-risk Key — Typically an "operator" key that only opens a few doors (but not an exterior door)
b. Medium-risk Key — Typically an interior-only sub-master or departmental master key
c. High-risk Key — Typically a building master, restricted access key, high-security key, or one that opens an exterior door

IV. POLICY

A building's key and lock system design will be developed only by the Lock Shop and in conjunction with the person from the affected department designated by the department head, dean, or chairperson. Structurally the system may have

four potential levels: (1) building master key; (2) departmental master key; (3) departmental sub-master key; and (4) operator key.

No lock (with the exception of roof access points, service closets, electrical-mechanical spaces, and construction areas) will be allowed to be "off the building master" system without prior authorization from the executive director of public safety. With the exception of buildings not having card access on exterior doors, all exterior doors, and all dormitories with keyless-style locks, will be cored with a high-security core unless otherwise authorized by the director of public safety.

Authorization for the Issuance of Keys – An internal control procedure is needed by every department that requests, holds, or issues keys. The University may periodically conduct an audit of how well a department is complying with this policy. Documented authorization for keys to be issued shall be as follows:

High-risk Key:

High-security Key – Executive Director of Public Safety

Building Master Key – Executive Director of Public Safety and department head, dean, chairperson only (no exceptions)

Restricted Access Key – Designated person responsible for the area secured (O.I.T., Facilities, departmental lock and key coordinator, etc.)

Medium-risk Key:

Building Sub-master Key – Department head, dean, chairperson only (no exceptions)

Low-risk Key:

Operator Key – Department's lock and key coordinator

Financial Responsibility – When any key from any risk category is determined to be unaccounted for, the Security Advisory Group will make a determination as to financial responsibility. The determination will be based on the facts and circumstances involved, to include whether or not the key holder of record was in compliance with this policy, and otherwise exercised reasonable and prudent care of the unaccounted for keys. As a general rule:

a. If a University employee is determined to be responsible for lost/missing/stolen keys, that employee's department may bear all costs associated with the unaccounted for keys (including, but not limited to the cost to re-key affected areas);

c. If an employee of a contractor/construction design firm/professional services firm in possession of a University key is determined to be responsible for lost/missing/stolen keys, that firm may bear all costs associated with the unaccounted for keys (including, but not limited to the cost to re-key affected areas.)

De-authorization for a Key – When a key is no longer needed, or the key holder is de-authorized from having one or more keys, the key holder should return the key(s) promptly to the Lock Shop, or to their department head, dean, chairperson, or their designated lock and key coordinator. Key holders or local key coordinators are not to transfer "high-risk" keys to another employee. Such re-issuance will only be processed by the Lock Shop.

Separation from Employment – When faculty or staff are terminated by the offices of the Dean of the Faculty or Human Resources as part of a disciplinary action, those offices have responsibility to retrieve any issued University keys, which are to be returned to the Lock Shop. When a member of the University community is departing from the University under circumstances other than a disciplinary action, the local department has the responsibility to get back any University keys.

Local Key Boxes – Use of local key boxes to house unassigned keys which are controlled by departments is permitted. However, local key boxes shall be of a type and style as specified by the Security Advisory Group. Additionally, the University may conduct periodic audits of any local key box to ensure compliance with this policy.

Policy Exceptions – While this policy addresses a wide range of access issues relating to keys, it is unlikely that every possible variable has been considered. Any exceptions to this policy must be submitted in writing to the executive director of public safety for consideration.

V. PROCEDURES

Issuance of Keys – Keys will only be issued on an indefinite basis to members of the University community -- faculty, staff and students (i.e., not contractors, etc.). There must be a written authorization from the appropriate level for key issuance. To ensure a minimum amount of risk from lost keys, each department will be issued no more than two (2) building master keys to their building. Any amount greater than two will be considered on a case-by-case basis by the executive director of public safety.

Keys are picked up and signed for at the Lock Shop customer service window at the Facilities Department. Operator-level keys may be picked up by any responsible person authorized to do so by the department local key coordinator, but all medium-risk and high-risk keys must be picked up and signed for by the person who will ultimately control and be responsible for the key(s). Students who will be issued keys are to pick up their keys from their local department.

Any employee receiving a key will be required to identify themselves by swiping their Princeton University identification card at the Lock Shop customer service window. Students will not be allowed to pick up keys not being issued to them personally.

Tracking of Keys – The Lock Shop will track the issuance of all "high-risk" keys, as well as temporary keys that are signed-out. Department heads, deans, and chairpersons (or their designate) will be responsible for tracking the issuance of, and ensuring the return of all keys in their control, no matter what risk level (i.e., including medium- and low-risk keys as well as high-risk keys). The Lock Shop is available as a resource for best practice key control.

Temporary Key Issuance – Because of the unique short-term nature of temporary access needs, the high volume of such transactions, and in the interest of timeliness for key delivery, the standard authorization procedure does not apply to temporary key sign outs from the Lock Shop customer service window. In all cases of temporary key sign out, a defined return date is required and must be complied with, or sign out privileges may be revoked.

To ensure an appropriate level of key control for these unique transactions, the following procedures apply:

a. For employees – a University ID card swipe, and log entry with signature and date of return;

b. For non-employees – the Princeton University employee responsible for the work being done by the non-employee shall sign out the key(s) (with a University ID card swipe and log entry with signature and date of return by the employee) and shall return the key(s) promptly upon job completion. Non-employees will not be granted unsupervised access to buildings where students and/or children are housed.

Note: If a department has a non-university employee who has a frequent/regular need for temporary key sign outs, but finds it impractical for the employee to sign keys in/out each time, the Princeton employee can submit a *Non-Employee Key Control Plan* to the Security Advisory Group that, if approved, would allow the non-employee to sign keys out/in under the same requirements as an employee for the agreed upon time frame.

Unaccounted for Keys – Unaccounted for (lost/missing/stolen) keys shall be reported to the Department of Public Safety as soon as possible after the key holder determines a key is missing. The Security Advisory Group will determine whether or not a re-coring of the affected building(s) and/or locks will be necessary as a result of any keys that are lost/missing/stolen. The daily Department of Public Safety crime report includes information about lost/missing/stolen keys.

VI. ROLES and RESPONSIBILITIES

Lock Shop – The Lock Shop is responsible for processing key requests, and ensuring proper authorization is in place for creating, issuing, and replacing keys for employees. The Lock Shop is also responsible for tracking the issuance of all "high-risk" keys, and for reporting the loss of all unaccounted for keys of which they become aware. The Lock Shop will also serve as an advisory resource to departments on best practices for key issuance and control.

Security Advisory Group – This standing University committee reviews, approves/denies certain key requests, and determines the proper course of action when keys become lost/missing/stolen.

Executive Director of Public Safety – The position responsible for reviewing and approving/denying all requests for a "high-risk" key.

Key Holder – A key holder is the person to whom one or more keys are issued, or for which they are in possession. By possessing a key, the key holder must not compromise the security of any area/building.

Key holders must return all University keys when requested, or upon termination of employment (per University policy 4.0.2, *Return of University Property*), promptly report lost/missing/stolen keys, and take reasonable and prudent care of University keys at all times.

A key holder should not:

a. Loan out keys
b. Transfer keys
c. Duplicate keys
d. Alter lock/access/alarm mechanisms
e. Prop open secured doors
f. Non-employees holding high-risk keys should not take them off campus, and should return them to the Lock Shop each day
g. Admit unauthorized persons into University buildings/facilities

Department Heads, Deans, Chairpersons – Department heads, deans, and chairpersons should ensure that the fewest number of keys and the lowest-level of keys possible are issued to faculty, staff and students in their departments. Issuing high-risk keys for convenience is discouraged. Additionally, they have the following responsibilities relating to key control within their department:

a. Develop a local department-specific key control procedure consistent with the requirements of this policy. At a minimum, the policy should include a log of who was issued the key, issue date, key number, reason for holding the key, building name, and return date;

b. Develop an appropriate policy to ensure the return of University keys from persons on disability or a sabbatical;

c. Perform the function of the local lock and key coordinator, or assign a person responsible for performing this function.

Departmental Lock and Key Coordinator – The person within each department authorized by the department head, dean, or chairperson to be responsible for requesting and authorizing keys, requesting lock changes, issuing and tracking keys within the department, reporting keys that are unaccounted for, managing a local key lock box (if department is authorized to hold unassigned "high-risk" keys), safeguarding unassigned keys, and for ensuring the return of keys no longer authorized by the department. Department coordinators may establish a policy to collect a cash deposit for all keys issued. Cash handling shall be consistent with the *Cash and Check Handling Policy* as published by the Office of Finance and Treasury.

Office of the Dean of the Faculty and Office of Human Resources – The offices of the Dean of the Faculty and Human Resources are responsible for notifying the Lock Shop of departing faculty and staff in a timely manner, and for ensuring the return of issued keys from individuals departing University employment.

VII. RELATED POLICIES

University Policy 4.0.2 – Return of University Property:
http://www.princeton.edu/hr/policies/termination/4.0/4.0.2/

University Policy – Cash and Check Handling Policy:
http://finance.princeton.edu/policy-library/cash-handling-receipts-1/cash-and-check-handling-p/?sq=cash and check handling policy

VIII. UPDATE LOG

Approved, August 1, 2013