COLLEGE of CHARLESTON

OFFICIAL POLICY

8.1.6	POLICY ON KEYS AND OTHER BUILDING ACCESS DEVICES	7/26/2016

Policy

COLLEGE OF CHARLESTON
POLICY ON
KEYS AND OTHER BUILDING ACCESS DEVICES

1.0 PURPOSE OF POLICY

The purpose of this Policy is to provide for increased security over physical access to College Real and Personal Property. Such increased security will serve to better protect students, faculty, staff, College invitees and all other persons permitted by law, or otherwise authorized by the College, to enter College Real Property and will improve the College's ability to safeguard College Personal Property and other Personal Property used, stored, or carried onto College Real Property. While the College intends to improve its management over the use and availability of keys and other building Access Control Devices to further these security interests, it intends to achieve this purpose in a manner that will not deny appropriate access to work areas or to academic or research areas by students, faculty, employees, and others who have a legitimate reason to access such areas.

2.0 POLICY STATEMENT

It is the Policy of the College to permit access to College Real Property, and to those Physical Facilities located on such Property, only to those individuals who have a legitimate reason for entering or entering and remaining on College Property. The College shall also protect, insofar as practicable, all such individuals, College Personal and Real Property, and the personal property of others lawfully on its premises. Lastly, it is also the Policy of the College to further these compelling interests, in part, through the management of building keys and other building Access Control Devices.

3.0 APPLICATION

This Policy applies to all members of the College Community.

4.0 DEFINITIONS

The following terms shall have the meaning ascribed next to each:

4.1 **"Access Control Device" –** any key, code, card, scanner or other device, whether mechanical or electronic, that is intended by the College to control, monitor, or manage ingress and egress to a Physical Facility or any part of a Physical Facility.

4.2 **"Campus-Wide Access Security Plan" –** is the Plan that is further described in Section 5.1 of this Policy.

4.3 **"College Community"** – shall mean the students, faculty, employees, officers, trustees, volunteers, and invitees of the College who are on College Real Property.

4.4 **"College Personal Property"** – shall mean property that is owned, leased, or otherwise in the lawful possession of the College, other than real property.

4.5 **"College Real Property"** – shall mean College owned or leased land and all additions or improvements to such land, if any, including but not limited to, buildings, structures, and anything permanently affixed to the land.

4.6 **"Part Time Employee"** – shall mean an employee who is regularly scheduled to work less than 37.5 hours a week.

4.7 **"Personal Property"** – shall mean anything other than real estate that is legally used, stored on, or carried onto College Real Property.

4.8 **"Physical Facilities"** – shall mean buildings, building additions, and other structures located on College Real Property that have a means for ingress and egress by which persons may enter and exit the facility.

4.9 **"Security Access Code"** – shall mean a way of access to a Physical Facility through the use of an electronic device requiring a code, or through some mechanical means also requiring a code (such as a combination lock), other than by the use of a traditional mechanical key.

4.10 **"Volunteer"** – shall mean any person who, of his/her own free will, provides goods or services, without any financial gain, to the College on either a continuous or intermittent basis and otherwise qualifies as a "Volunteer" under S.C. Code Ann. § 8-25-10.

4.11 **"Non-Restricted Access Areas"** – shall mean any space on campus that is generally open to the public during regular business hours of the College.

5.1 CAMPUS-WIDE ACCESS PLAN

5.2 Formulation. From time to time, the Executive Vice President for Business Affairs shall formulate, or cause to be formulated by experts in the field, a Campus-Wide Access Security Plan (the "Plan"). Among other things, the Plan shall contain a risk assessment and site survey analysis of College Facilities, solutions to noted security deficiencies, and a time-phased schedule for implementation of agreed upon solutions. For each Physical Facility, or group of like Facilities, the Plan shall identify the recommended numbers, types, and locations of various Access Control Devices, alarms, and remote monitoring technologies, and shall take into account the population characteristics of each Facility, the value and nature of items stored, used or carried into such Facility, and the placement of security cameras. The Plan shall be exempt from public disclosure pursuant to S.C. Code Ann. §30-4-40(a)(3)(D).

5.3 Management of the Plan. The Plan shall be managed by the Director of Public Safety, subject to the administrative authorities of the Director, Physical Facilities pursuant to Section 5.3. As further described in Section 7.1(a), such management shall include planning, organizing, and directing the effort to evaluate and install building Access Control Devices (in cooperation with the Office of Procurement and Supply) and making recommendations for such revisions of this Policy as the Director may believe appropriate. Such recommendations shall be made to the Executive Team, through the Executive Vice President for Business Affairs, in accordance with the College Campus Wide Policy Making Procedures.

5.4 Administration of the Plan. The Plan shall be administered by the Director, Physical Facilities to the extent that such Plan addresses the use of keys or other mechanical entry devices. As further described in Section 7.1(b), such administration shall include controlling the production, storage, and issuance of keys; the replacement or rekeying of lock cylinders; the acquisition of replacement keying systems; the maintenance of accurate records; and the cataloging of and adherence to key system authorizations. The administration of the Plan with respect to electronic security access devices shall be as provided for in Section 10.0.

5.5 Interim Measures. During the interim period (before the Plan is developed), the Physical Plant Lock Shop will consult with the College Chief of Police and/or the Physical Plant Director on requests that are considered unusual, extraordinary, or questionable. To the extent possible, elements of this proposed policy will be utilized in decision-making.

6.1 IMPLEMENTATION PRINCIPLES

6.2 Principles. Subject to the provisions of Section 6.2, this Policy shall be implemented in accordance with the following principles dealing with access to College Real Property:

(a) Secure Facilities. All College building perimeter doors will be secured by either key, electronic security access devices, other Access Control Device, if such a system should be developed and employed by the College, centralized security access control system. All requests for exceptions to this rule must be submitted, in writing, to the College Police Chief and the Physical Plant Director or their designees for approval. The College Police Chief and Physical Plant Director will consult on all such requests.

(b) Unrestricted Access. Public Safety (campus police and Fire and EMS) and the Director of Environmental Health and Safety shall have unrestricted access to all Physical Facilities for reasons related to safety, security, and health.

(c) Employee Access. Employees shall be given access to and from their workstations and all surrounding Non-Restricted Access Areas during regular business hours. Full-time employees who are exempt under the provisions of the Fair Labor Standards Act (e.g. managers, supervisors, teachers and other professionals) and adjunct and visiting faculty will be provided access to and from their workstations at such other times as may be needed to perform the requirements and responsibilities of their respective positions. Full-time employees who are non-exempt under the Fair Labor Standards Act shall be authorized access to and from their workstations outside of normal work hours only as approved by their immediate supervisors. A part-time employee or a volunteer will not be permitted to access an assigned work area during non-regular work hours unless that part-time employee or volunteer: (a) has a legitimate interest to be present at such hours and the relevant supervisor (at the level of a dean, vice president or higher) signs a certification of need for access during non-working hours and why the relevant services cannot be performed during regular working hours; or (2) is under the direct supervision of an onsite full-time employee during such non-regular work hours.

(d) Students. Students who are not subject to a disciplinary directive to stay off College Real Property or a portion of such Property (or otherwise restricted pursuant to Section 6.2) shall be given access to and from non-restricted areas of College Real Property as are needed to enjoy the full benefits of a College of Charleston educational and community living experience in accordance with the Key and Lock Policies and Procedures established by Office of Residence Life and Housing.

(e) Vendors. Vendors and their employees and other representatives shall be given access only to those areas of College Property on such days and at such times as are needed for the provision of their services or the supply of their goods.

(f) Invitees. Invitees of the College may enter and/or remain on College Property during such times and for such purposes as are approved by the College. Keys or other Access Control Devices should not normally be made available to invitees of the College unless such keys or other Devices are: (a) needed for access to approved guest housing accommodations; or (b) approved at the level of a dean, vice president, or higher upon the presentation of justification that such access to Physical Facilities is needed for legitimate College purposes outside of normal work hours.

(g) General Public. Members of the public may enter areas of College Property for a legitimate and legal reason, provided that, such presence in an area: (i) is not disruptive; (ii) does not interfere with the work of the College or the education or living experiences of our students; (iii) does not constitute an invasion of personal privacy; (iv) does not expose confidential records of the College to public visibility; (v) does not constitute a unreasonable risk to the health or safety of the College Community; (vi) is incompliance with all other policies and practices of the College that may require pre-approval and/or time, place or manner restrictions.

6.3 Notices and Stay-Away Orders. No person, regardless of position, who is subject to a barring notice issued by the College, or who is subject to a "stay-away" or other order issued by a

court of competent jurisdiction, shall be permitted on College Real Property in contravention of such notice or order.

7.1 MANAGEMENT AND ADMINISTRATION OF KEYS

7.2 Responsibilities.

(a) Department of Public Safety – The Department of Public Safety is responsible for the security of College Real and Personal Property and shall inform the appropriate manager, at a level of vice president, dean or higher, of any condition (such as unlocked doors or doors that are improperly propped opened) that may constitute a security risk. The Office of Public Safety shall also monitor all security devices including, but not limited to, security cameras.

(b) Physical Plant – Physical Plant shall be responsible for the installation of mechanical locks and the production and distribution of keys for Physical Facilities that are not otherwise installed or issued by independent contractors retained by the Office of Procurement and Supply for such purposes. In accordance with Section 10.0, Physical Plant shall also keep records of keys issued to all College employees and maintain a security software system which will record building key data and employee key records.

(c) Key Managers and Security Access Representatives – These persons (See Section 8.0) will maintain records of key distributions for the buildings and/or departments under their assigned responsibilities.

(d) All Members of the College Community – Upon reasonable suspicion, each member of the College Community shall promptly report a lost or stolen key or compromised Security Access Codes to the Department of Public Safety. Potential compromises to the security of classroom access codes should be reported to the Registrar's Office.

7.3 Levels of Regulated Access.

(a) General Rule. A person will be issued that level of access to Physical Facilities of the College through the issue of keys or Security Access Codes that is at a level commensurate with their position and their assigned College duties and responsibilities. Except as provided in subsection (c) of this Section 7.2, such decisions will generally be made by the supervisor in the management chain at a level of dean or vice president or higher.

(b) Types of Access.

(1) Campus-Wide Master Key or Access Control Device: Provides total access to all buildings within a particular system on campus. As warranted, exceptions can be made based on operational needs (e.g. College bookstore) to having access controlled through the campus-wide master. Such exceptions are at the discretion of the appropriate Executive Vice President. Public Safety will maintain the right to access all campus space at all times for safety and security reasons.

(2) Building Master Key or Access Control Device: Provides access to an individual building and all spaces with the exception of mechanical and communication spaces within that building.

(3) Building Exterior Key or Access Control Device: Provides access to an individual building with exception to the mechanical and communication spaces within that building.

(4) Building Sub-Master Key or Access Control Device: Provides access to a group of rooms within a building.

(5) Individual Room Key or Access Control Device: Provides access to a room/office within a building.

(c) Restriction. Authorization for the issuance of a Campus Wide Master Key or Access Control Device may only be granted by the President, the Executive Vice President for Business Affairs, or the College Chief of Police, and will be restricted to security, safety, environmental health and selected senior maintenance personnel only. The Chief of Police, the College Director of Environmental Health and Safety, and the College Director of Physical Plant shall be provided such a key under this Policy.

(d) Small Facilities. Notwithstanding any other provision of this Policy to the contrary, only one key will be issued per authorized user for a Physical Facility having 20 or less rooms. The key will allow access to the building exterior and to the individual room. Exceptions to this limitation may only be made granted by the Executive Vice President for Business Affairs upon a showing that additional keys are needed to further a legitimate interest of the College.

7.4 Access Approvals.

(a) Full Time Permanent Employees – Full time employees will be issued keys or Security Access Codes or other Access Control Device upon the recommendation of a supervisor in their management chain at the level of a dean, a vice president, or higher.

(b) Students – Those students who are Campus residents will be given keys or Security Access Codes, as appropriate, to their assigned residence facility and room. Students who are also part-time employees or volunteers may also be given access for Facilities pursuant to subsection (c) of this Section 7.3. In all other cases, students will not be given access unless it is to a Facility being used by such students for approved academic purposes or student activities, or access is needed by an approved student organization for its meetings or activities. Decisions made under the immediately preceding sentence shall be made by the Executive Vice President for Student Affairs or his/her designee or the Executive Vice President for Academic Affairs or his/her designee.

(c) Part-Time Employees, Uncompensated Faculty and Other Volunteers – These persons will be issued keys or security Access Codes only if: (a) the responsibilities of the position must be routinely performed during other than regularly scheduled work hours; (b) the immediate

supervisor or other appropriate responsible College employee has a reasonable method to assure that work is actually being performed during such times; (c) the recommendation for the issuance of keys is made by a supervisor in the management chain at the level of a dean, a vice president, or higher; and (d) the uncompensated faculty member or employee who is the subject of the request undergoes a successful background check under the College's Background Checks Policy.

(d) Vendors – Vendors will be issued a key or other Access Control Device only when essential to the performance of their contractual obligations, as determined by the appropriate College employee charged with contract administration responsibilities and the Director of Procurement and Supply, and the vendor's employee entrusted with a key undergoes a successful background check under the College's Background Checks Policy.

7.5 Responsibilities of Key Holders and Security Access Codes.

All College key holders and those persons with a Security Access Code assume the responsibility for the safekeeping of the key/Code and may be required to a sign a statement acknowledging that fact prior to the issuance of a key or a Code. The failure to demonstrate a continuing ability to meet such a responsibility will result in a declination to provide any key or Access Code to the individual. Any loss sustained by the College or to a member of the College Community resulting from the negligence of the person who was originally issued a key or Security Access Code may result in the immediate consideration of disciplinary action against that person and a claim by the College for restitution from such individual.

8.1 DESIGNATIONS AND DUTIES OF KEY MANAGERS OR SECURITY ACCESS REPRESENTATIVES

8.2 Designation. Each Executive Vice President shall designate one or more Key Managers or Security Access Representatives for those buildings and offices that are under her/his primary control. In all cases of shared use or conflicting opinions, the Executive Vice President for Business Affairs will decide the matter and will, in addition, assure that each building has a Key Manager or Security Access Representative.

8.3 Qualifications. A Key Manager or Security Access Representative must be a full time employee of the College and may be required to undergo a successful background check under the College's Background Checks Policy. Such an employee may be the Manager or Representative for more than one building or related groups of buildings.

8.4 Duties of Key Manger or Security Access Representative. Duties include the following: key issuance (as well as other Access Control Devices) and collection, along with related paperwork and record keeping; and acting as department/unit liaisons with the Physical Plant Lock Shop, Public Safety, and building occupants.

9.1 PRINCIPLES DEALING WITH THE DISTRIBUTION OF KEYS

9.2 Keys. Keys for College Property shall be issued, replaced, transferred, and collected in accordance with the principles stated in this Section 9.0 and such operating procedures as may be promulgated from time to time by the Office of the Executive Vice President for Business Affairs. The principles referenced in the preceding sentence are as follows:

(a) Missing Keys. Lost or stolen keys will not be replaced until a report has been filed with Public Safety. Keys will be replaced when a copy of a Public Safety report has been provided to the Physical Plant Lock Shop.

(b) Rekeying. Lost or stolen keys for rooms or offices containing high dollar value items, laboratory chemicals, biological agents, or other dangerous or hazardous materials, sensitive financial information, personally-identifying information on a significant number or persons, or privileged materials may require rekeying the lock, as determined by the senior manager (at the level of a dean, vice president, or higher) having responsibility for that area.

(c) Replacements. All requests for additional keys or replacement keys must be submitted by a Key Manager or Security Access Representative to the Physical Plant Lock Shop.

(d) Duplications. A request for key duplications must be submitted to, coordinated with and performed by the Physical Plant Lock Shop. Any other method of duplication is prohibited.

(e) Unauthorized Locks. No lock may be purchased with College funds or installed on a College building or on College Real Property in contravention of this Policy. Locks installed in contravention of this Policy will be removed at the expense of the department who purchased or installed the locks.

(f) Surrender of Keys. College keys shall be returned when an employee terminates employment, retires, resigns, transfers between departments, or changes room assignments. Keys issued to a vendor must be surrendered when no longer essential to performance of the contracted work as determined by the appropriate College employee charged with contract administration responsibilities and the Director of Procurement and Supply.

9.3 Operating Procedures. The Executive Vice President for Business Affairs may promulgate such operating procedures as s/he may deem appropriate to implement this Section, provided that, such procedures do not conflict with any principle stated in Section 9.1.

10.1 RECORD KEEPING

10.2 Keys. Physical Plant will maintain records on all employees, volunteers, student workers, and vendors who are issued keys. These records shall be maintained in an electronic database and shall be current within 48 hours. The records shall contain, among other things, information on all

keys issued, duplicated, lost, stolen, returned, and transferred. The Department of Public Safety shall have electronic access to that data base.

(a) Reports. The Lock Shop will provide Key Managers/Security Access Representatives with reports of key records grouped by department as requested, and will work with the Key Managers/Security Access Representatives to maintain the accuracy of these records as changes occur.

(b) Inventories. The Executive Vice President for Business Affairs shall cause a physical inventory of keys to be conducted from time to time to ensure compliance with this Policy.

10.3 Security Access Codes. Physical Plant shall be responsible for maintaining complete records on all persons who have Security Access Codes to one or more buildings.

10.1 SPECIAL PROVISIONS FOR ELECTRONIC ACCESS CONTROL

10.2 Principles. Electronic access to certain Physical Facilities on College Property shall be managed in accordance with the principles stated in this Section 10.0 and such operating procedures as may be promulgated from time to time by the Department of Public Safety. The principles referenced in the preceding sentence are as follows:

(a) Cougar Card. Electronic access to certain Physical Facilities will be by electronic access. Members of the College Community and approved vendors are required to maintain a Cougar Card for such access.

(b) Responsibility. The Security Access Representative for the facility has the overall responsibility of ensuring that the building users are using the electronic access control system and shall ensure that all building users have valid Cougar Cards and appropriate clearance and access for their areas.

(c) Notifying Public Safety. The Security Access Representative for the facility is responsible for notifying Public Safety in the event that an electronic access system is compromised or is not functioning as intended.

(d) Keys to Electronic Access Facilities. No keys are issued to any Electronic Access Control doors except for specific personnel that are required to have such a source of back-up access. Such determination will be made by the College's Chief of Police and College's Physical Plant Director.

(e) Circumvention. Tampering with or attempting to bypass security on an electronically controlled or monitored door in any way, including but not limited to key bypass, propping, taping and/or dogging, is prohibited, except that, when needed to accommodate a legitimate Campus event or activity.

(f) Code Recipient's Duty to Report. The recipient of a Security Access Code shall be responsible for the security of that Code and shall promptly report any circumstance that the recipient reasonably believes has compromised the confidentiality of that Code to the Security

Access Representative for the facility.

10.3 Operating Procedures. The Department of Public Safety may promulgate such operating procedures as it may deem appropriate to implement this sections, provided that, such procedures do not conflict with any principle stated in Section 10.1.

11.0 PRESIDENT

Exceptions to this Policy, or to any provision herein, may be granted by the President at any time and for any reason s/he believes appropriate in the best interest of the College.

12.0 AMENDMENTS

This Policy may be amended in accordance with the College's Campus Wide Policy Making Procedures.

13.0 RESPONSIBILITY

The Department of Public Safety of the College and the Department of Physical Plant shall be responsible for the maintenance of this Policy

14.0 EFFECTIVE DATE

This Policy Shall become Effective 07/26/2016

a. ********************

Policy Manager and Responsible Department or Office

The Department of Public Safety is responsible for administering this policy, and the Physical Plant is responsible for managing the policy. The College Chief of Police will consult with the Physical Plant Director and Environmental Health and Safety Director to ensure the policy and procedures remain current to address business processes and the status of types of access control at the College of Charleston.

Purpose/Reason for the Policy

In August 2009, the Space Committee recognized the need to review current practices, procedures, and policies relating to access management and to make recommendations for process improvement. A small workgroup was formed with two primary outcomes: 1.) the need for a formalized access control policy and procedures and 2.) the need to hire a consultant to develop procedures and to provide a risk assessment with a prioritized plan for implementing new hardware and software. The policy was drafted with input from Academic Affairs, deans, Faculty Welfare Committee, Legal Affairs, Public Safety, Physical Plant, and Business Affairs. The policy provides the framework for a responsible system of access management at the College of Charleston and sets clear expectations for individuals who are assigned keys and/or access codes.

Departments/Offices Affected by the Policy

All departments will be affected by the policy. Those with primary responsibility for implementing, administering, and managing are: Business Affairs, Physical Plant, Public Safety, and Environmental Health and Safety.

Procedures Related to the Policy

The procedures will be developed after the policy is approved by the Executive Team. If a consultant is hired, he/she could be tasked with assisting with the development of business procedures.

Related Policies, Documents or Forms

To be developed.

Issue Date:7/26/2016 **Date of Policy Revision:7/26/2016**	**Next Review Date:10/26/2020**

POLICY APPROVAL
(For use by the Office of the Board of Trustees or the Office of the President)

Policy Number: 8.1.6

President or
Chairman, Board of Trustees _____ Date: 7/26/16