CRISWELL COLLEGE

Administrative Policy
Campus Access

Approved By: President
Date Approved: February 27, 2015
Effective Date: February 27, 2015

1. **Summary:** This policy establishes the procedures for the issuance and management of campus keys, key cards, and other access controls.

2. **Rationale:** This policy is necessary for the proper administration of campus access and, thereby, the safety of the College's campus.

3. **Entities Affected:** students, faculty, staff, residents, other parties granted access to campus

4. **Definitions:**
   individual key access: operates only one lock or a few specific locks in a designated area

   key access device: any form of access control and its access capabilities, including (but not limited to) keys, key cards, and key fobs as well as passcodes, passcode apps, and even biometric data as they apply

   master key access: operates all locks in a particular building or designated area

   sub-master key access: operates a limited portion of the locks that the master key access operates

5. **Policy:** Criswell College's facilities are to be used as fully as possible within the limits of reasonable security practices. To this end, all key access shall be issued on a need basis only to those persons requiring necessary, regular access to lockable areas on the College campus.

   Criteria for Issuing Key Access
   - Only a College president, vice president, department director, or department supervisor may initiate a key access request.
   - The College's Chief of Police, under the authority and direction of the Chief Financial Officer, must approve a key access request before key access may be issued.
   - The College president or a vice president must approve a request for master key access before master key access may be issued. Approval must be received from the director or department supervisor overseeing the facility or area the key access device will gain access to *if* it makes accessible a facility or area not under the regular purview of the department head or vice president filling out the *Campus Key Access Request* form.
   - A key access request shall be approved for the lowest level key access possible that still meets the accessibility need. The issuance of sub-master key access or master key access should be avoided whenever possible.

- Approval of a key access request is based on the following factors:
  - The relationship to the College of the individual for whom key access is being requested (student, staff member, faculty, member, contractor, etc.);
  - The College-related responsibilities of the individual for whom key access is being requested;
  - The frequency with which access to a designated area is needed by the individual for whom key access is being requested;
  - The availability of the designated area to which access is being requested, including the general times the designated area is unlocked;
  - The degree to which access to a designated area is needed or necessary. The Event Request system is preferred and to be utilized whenever possible for meetings or events being held within area(s) not under the responsibility of the department considering a key access request.

Key Access Request Process

- A key access request must be initiated by submitting a *Campus Key Access Request* form to the Campus Police Department. A separate *Campus Key Access Request* form must be filled out for each individual needing access to certain areas. Key access devices for part-time employees or key access devices shared within a department must be assigned to the department's highest-ranking employee or a duly appointed representative (e.g., an employee's supervisor).
- Employees submitting a key access request must make arrangements to pick up any issuable key access devices and must sign the *Key Access Log* form before such devices may be issued. No more than one key access device to a designated area may be issued to any one individual.

Key Access Holder Responsibilities

- Key access holders must maintain personal possession of their issued key access devices and must not lend their issued key access devices to others for any reason.
- Individuals must immediately report any broken, lost, or stolen key access devices that were issued to them to the Campus Police Department. Key access devices that are found by someone other than the key access holder must immediately be submitted to the Campus Police Department or alternatively, specifically in the case of College-issued ID cards, the Student Services Office.
- Key access holders using their key access outside of normal operating hours must ensure that all access points are closed and locked upon entering and leaving campus facilities.
- Key access holders must supervise any individuals for whom they have provided campus access by using their issued key access devices.
- All issued key access devices are the property of Criswell College, must not be duplicated, and may be reclaimed by the Campus Police Department at any time.

Returning Key Access

- Key access holders must immediately return their issued key access devices to the Campus Police Department (or alternatively, specifically in the case of College-issued ID cards, the Student Services Office) if their employment at the College is terminated, if they transfer to another office or department and no longer need the access a key access device provides, or if their College-related responsibilities change so that they no longer need certain key access.
- The Campus Police Department shall record all returned issued key access devices in the key access holder's *Key Access Log* form.

6. **Procedure:**
   a. **Implementation:** The Chief of Police is responsible for maintaining procedures by which this policy can be implemented.
   b. **Responsibility for Compliance:** Chief Financial Officer
   c. **Notification:** This policy will be posted on the College's website.
   d. **Policy Review:** This policy will be regularly reviewed according to the College's policy review procedure.

For the Office of the President only:

Policy version: 2.0	Policy number: 2.030
Related policies:	

Policy History

Version 1.0	October 21, 2014
Version 2.0	February 27, 2015