

**Cochise College
Administrative Policy**

Category: Fiscal Management

Policy Number: 2013

Title: Key Control

The President is requested to authorize, establish and enforce a key control policy for all campuses and centers of Cochise College. This policy will include authorization, distribution, control, maintenance, responsibility, and operational procedures.

Procedure 2013.1

Key Control

1. Building keys will be issued only when there is a demonstrated need for persons to have access to College facilities. The fact that a person is employed in an area may not be sufficient justification for the issuance of a key.
2. Issuance of building keys is limited to authorized employees only. Requests for keys must be submitted on a Key Request Form, and approved by the appropriate College official(s).
3. Issuance of keys is restricted to full-time Cochise College employees. Exceptions must be approved by the College President.
4. Cochise College Physical Plant Department is responsible for issuance, maintenance, record keeping, and other functions necessary to maintain the College key system.
5. Keys will be issued only after a completed Key Request Form, with the required approval signatures, has been processed through the district Human Resources and Physical Plant offices.
6. To receive a replacement for a broken key, all parts must be presented. If portions of the key are still in the lock, the district locksmith will recover. If portions of a key are missing, it will be treated as a lost or stolen key.
7. Lost or stolen keys must be reported to Security immediately to ensure security of the affected area. Request to replace lost or stolen keys must be made by completing a Lost or Stolen Key Replacement Form. The form must have the appropriate authorization for the missing key. In addition, a copy of the Lost Key Report filed with Security must be attached to the Replacement Form. A replacement charge will be charged to the requesting department, and will include the cost of making a key and cost of necessary re-keying to maintain security of the affected area(s). Cost

may range from \$10.00 to \$500.00.

8. Duplicate keys will not be issued. Only one key type or numbered key will be issued to an individual. No single-function key will be issued to individuals who have been assigned a master key that gains access to the same area.
9. Persons assigned building keys will be held responsible for the security of the area and all property within that area. Persons requiring access to an area after normal working hours, or persons not having their keys with them, will be required to check in at the Security office to identify themselves and to be checked for authorized access into the area. Entry and departure dates and times will be recorded by Security.

Procedure 2013.2 Key Return

1. All keys will be returned to the Key Control Office upon departure of any employee in possession of a key (or keys). The Human Resources Office will be responsible for obtaining clearance from the Key Control Office, indicating that departing personnel have returned all keys. Clearance will be required prior to approving separation actions and issuance of final payroll checks for departing employees.
2. Separations include (1) sabbatical leave, (2) termination/resignation, (3) leave, long-term illness, vacation, or other absence, for any reason, anticipated to exceed 90 days.

Procedure 2013.3 Loan of Keys:

Keys shall be issued for the use of the authorized requestor only. Loan or use of keys by others is strictly prohibited. Misuse of keys, or keys found in possession of unauthorized personnel, may result in confiscation and denial of reissue.

Procedure 2013.4 Key Audit

All keys will be inventoried annually to enable all approving authorities to review and evaluate building access requirements, and to ensure the accuracy of district and campus records. The audit will be coordinated prior to the faculty departure at the end of the spring semester. Key audits may also be requested by vice presidents, department heads, and Security, should their areas of responsibility be compromised.