Issuance, Usage, and Accountability of Keys & Electronic-Controlled Access

Purpose:

The purpose of this policy is to promote the security of College facilities and personnel and provide appropriate access to College property for authorized individuals. The policy describes key issuance requirements and responsibilities.

Scope:

This policy applies to all keys, key fobs or access cards issued for Dyersburg State Community College. This policy applies to all persons who are issued Dyersburg State Community College keys, fobs, access codes or other security tokens in the performance of their official duties or are responsible for the issuance and control of security tokens and keys.

Policy:

The Director of Physical Plant is responsible for the issuance and control of all keys (and key fobs or access cards), and for the control and maintenance of lock cylinders. The basic issue/control document will be the DSCC Key Request Form. Issuance of a key or key fob will be authorized by the requestor's direct supervisor and approved by the Vice President for Information Technology and Facilities Management on the Key Request Form.

The individual to whom keys (or key fobs or access cards) are issued is known as a key holder. Key holders are responsible for the use of their assigned keys (or key fobs or access cards) and shall not transfer them to another individual. Key holders shall not leave doors unlocked during hours when the facility is normally closed. Key holders shall not unlock buildings or rooms for others unless the individual has a valid reason for access as approved by the Director of Physical Plant. Key holders shall return any key issued to them to their direct supervisor or the Director of Physical Plant when requested by the College and report any lost keys as soon as the loss is known. Damaged keys must be returned to the Director of Physical Plant for replacement. In the event an employee is no longer employed with DSCC any keys issued must be returned to Human Resources or the Director of Physical Plant. (Human Resources will return the keys to the Director of Physical Plant.) If an employee changes room assignments and a new key request is processed, the employee must return the original key(s) to the Director of Physical Plant.

Holders of master keys shall not unlock or access spaces that are specifically assigned to an individual employee (such as offices, suites, and closets) without written consent from the employee who is assigned to the space or from the employee's direct supervisor. (Supervisors shall retain access to all their direct reports' offices/assigned spaces without needing written approval.) Employees whose job functions require regular access to spaces that are specifically assigned to an employee (such as information technology, maintenance, and custodial staff) are not required to obtain consent from the employee when performing their job duties. Classrooms, laboratories, and other common spaces are not spaces that are specifically assigned to an individual employee.

Any keys issued to adjunct faculty, or to full-time faculty for shared office space, must be returned by the end of the term. No key will be duplicated except by approval and control of the Director of Physical Plant. Exceptions to the policy: The Security vendor will utilize one master key per officer/campus/center as needed. The Security vendor will be given access to a lockbox system to exchange the keys during shift change if necessary. Alarm codes and key fobs will be issued to individuals on an as needed basis. For other vendors and contractors, keys will be issued to individuals with particular instructions regarding their company's responsibilities for returning the keys at the end of the assignment. A trace file will be kept by the Director of Physical Plant for these vendors and contractors.

Compliance:

Violations of this policy resulting in misuse of keys, unauthorized access to College facilities, or unauthorized disclosure or distribution of access codes, fobs or keys may subject individuals to legal and/or disciplinary action, up to and including termination of employment or contract with the institution or, in the case of students, suspension or expulsion from the institution.

Definitions:

Key fob – a small RFID hardware device that can be programmed to control access to a physical space. Also known as a *hardware token*, a key fob provides on-device, one-factor authentication to facilitate access to a keyless entry system.
Access card – a credit card sized RFID device that can be programmed to control access to a physical space.
Master key – a key granting access to many areas

Revision History:

Original Policy approved 4/1984. Policy revised 5/1999. Second Policy revision approved by Administrative Council on 01/30/2015. Third Policy revision approved by Administrative Council on 02/27/2018. Policy revision reviewed and approved by Admin Council on 04/27/2023. Policy revised March 2026; approved by Admin Council on 03/26/2026.