

## KAUA‘I COMMUNITY COLLEGE

### Facilities Access Control Policy and Procedures

#### 1. Purpose

Kaua‘i Community College (Kaua‘i CC) is committed to the safety of its faculty, staff, students, and visitors to maintain a safe, secure, and efficient learning and working environment. The primary objective of the Facilities Access Control Policy and Procedures is to balance the goal of maximum utilization and access to facilities with the need to control such utilization and access for the express purpose of 1) enhancing the personal safety for members of the campus community and, 2) minimizing potential loss or theft of property. This objective is supported through responsible access privilege control mechanisms for all campus-controlled facilities.

#### 2. Scope and Applicability

The Facilities Access Control Policy and Procedures applies to 1) all current and future sites, buildings, facilities, and other assets under the operational jurisdiction of Kaua‘i CC, 2) all access control systems installed in new construction or as part of any major or minor repair and maintenance project, and 3) all personnel affiliated with Kaua‘i CC to include its officers, employees, agents, or any person acting on behalf of Kaua‘i CC.

#### 3. Policy

The Facilities Access Control system will be used to promote and maintain the, a) safety and security of building occupants, b) protection of college property, and c) security of college records.

#### 4. General Guidelines

- A. All keys and electronic access cards are the property of Kaua‘i CC.
- B. The chancellor delegates to the vice chancellor of administrative services (VCAS) overall responsibility for granting access to Kaua‘i CC facilities, issuance of all keys and electronic access cards, and other related duties. The VCAS shall appoint a key control coordinator to assist him/her with the performance of these duties.
- C. Keys and electronic access cards will be issued to Kaua‘i CC faculty, staff, and administrators. At the discretion of their supervisor, student employees and members of the student government may be issued electronic access card(s).

- D. No person shall knowingly alter, duplicate, copy, or make a facsimile of any key or electronic access card to a lock of a building or property thereof without receiving permission from the VCAS.
- E. Keys or electronic access card transfers are strictly prohibited. Persons found in violation of this policy may have their access privileges revoked.

5. Facilities Access Control Responsibilities

A. VCAS Office Responsibilities

- i. Coordinate the installation and maintenance of interior and exterior door locks.
- ii. Coordinate the cutting and issuance of door keys and electronic access cards.
- iii. Maintenance of accurate records and controls to provide accountability for all keys and electronic access cards issued.
- iv. Establishment of policies and procedures that govern the issue and control of keys and electronic access cards.

B. Division/Department Head Responsibilities

Request keys or electronic access cards from the VCAS for faculty and staff employees assigned to their division.

C. Individual Key and Electronic Access Card Holder Responsibilities

- i. Assumes responsibility for the safekeeping and appropriate use of all keys and electronic access cards issued to them.
- ii. Key and electronic access cardholders are strongly encouraged to leave keys and electronic access cards in a secure location during non-working periods.
- iii. Keys and electronic access cards are only to be used by the individual who was issued the key or electronic access card and are not to be loaned or transferred to any other individual.
- iv. Authorized employees with electronic access and/or keys shall not give unauthorized persons access to a secured building or room.
- v. If a key or electronic access card is lost, it is the individual's responsibility to immediately report the loss to the key control coordinator.
- vi. Upon termination of employment or retirement from Kaua'i CC, keys and electronic access cards are to be returned to human resources during the exit interview.

- vii. Return keys to the key control coordinator when they are no longer needed.
- viii. Report and turn in any found keys or electronic access cards to campus security.
- ix. Report unauthorized persons or suspicious activities to campus security immediately.

#### 6. Key and Access Card Requests and Authorizations

Key and electronic access card requests must be made by the respective division or department head to the key control coordinator. Please allow 3 business days for the processing of all key and electronic access card requests.

#### 7. Key Identification (Excludes Electronic Access Cards)

Tags, markings, and any other forms of identification that refer to Kaua'i CC, or a specific building/room at the college, or in any way indicate the purpose of the key, should not be attached to the key. The only identifying marks on the key will be the characters/numbers stamped on the key by the operations and maintenance office.

#### 8. Key and Electronic Access Card Replacements

- A. Non-functional or worn keys or electronic access cards will be replaced at no charge. Defective keys or electronic access cards should be returned to the key control coordinator for disposal.
- B. Lost or stolen keys and electronic access cards may be replaced at the discretion of the VCAS based on the severity and frequency of the incident. Affected employees may appeal the VCAS's decision in writing to the chancellor, with the chancellor's decision being final.

#### 9. Key Issuing Guidelines

For security and key control purposes, the key and electronic access card issuing guidelines below will be followed:

- A. Campus Security Personnel: Electronic access cards to all external doors; master key for all offices, laboratories, classrooms, workshops, and studios.
- B. Administrators, faculty (including lecturers), and staff: Electronic access card to external door(s) leading to office suites, if applicable; key for own office or office suite. Keys to laboratories, workshops, and studios may be issued to faculty and staff whose assigned duties require the use of those spaces at the discretion of the VCAS after consulting with the Vice Chancellor for Academic Affairs. Affected employees may appeal the VCAS's decision in writing to the Chancellor, with the Chancellor's decision being final.

- C. Operations and Maintenance Staff: Electronic access card to external doors as assigned duties require; key for offices, classrooms, laboratories, workshops, and studios as assigned duties require.
- D. Student workers: Only if impractical otherwise.
- E. Volunteers: None.

#### 10. Temporary Keys and Electronic Access Cards – Contractors and Service Providers

Operations and maintenance staff will either notify campus security to provide access, or request a key or electronic access card to be issued through the key control coordinator.

#### 11. Building Schedules and Electronic Access Cards

- A. Each campus building may have its own schedule for opening and closing external doors as determined by the appropriate dean or division chair. Most buildings/offices will be open from 7:45 a.m. until 4:30 p.m., Monday through Friday excluding holidays and designated break periods.
- B. When the building is closed, the electronic door locks will automatically engage. On Saturdays, Sundays, and holidays, most buildings will be scheduled closed, unless special events are scheduled which require use of specific buildings and rooms. Special event requests for the electronic access system must be pre-arranged by submitting a facilities use form at least 10 business days in advance of the event.
- C. In the event of an emergency lockdown, all electronic locks will be engaged in the locked position to prevent entry into buildings. For the duration of the lockdown, electronic access cards will not allow access to buildings (Exception: first responders and certain campus officials who are given special lockdown access privileges). Building occupants will still be able to exit buildings during a lockdown.
- D. In the event of a power outage, a backup power supply will support the normal functioning of the electronic locks. Should the backup power supply fail, the electronic locks will fail secure, meaning they will remain in the locked position until power is restored. Building occupants will still be able to exit buildings during a power outage or if the locks are in the fail secure position.

#### 12. Campus Opening and Closing Procedures

- A. Operations and maintenance staff are responsible for unlocking doors to buildings and classrooms prior to the start of each instructional day.
- B. Staff and facility users are responsible for securing all doors that are not electronically locked on a schedule.

- C. Faculty are responsible for securing their office doors and any classroom doors for classes that end after 4:30 p.m. if they are the last user of the day.
- D. Campus security will ensure that all exterior doors are secured when the campus is closed.
- E. If an employee is locked out of a room or building, they should call campus security (245-8399 or X399 if using a campus telephone) for assistance. The employee will be required to provide identification and sign a security log form that will indicate the time, date, division, and building or room number to which the individual was provided access. Security will cross reference the faculty or staff member's name with a list provided by the VCAS office each semester.

### 13. Administration of Electronic Access Card System

The electronic access card control system will be administered and maintained by the VCAS office with technical support provided by computer services. Computer Services' responsibilities will include providing support for computer system maintenance, to include the coordination and installation of system hardware and software upgrades, as necessary. Computer Services is neither authorized to nor responsible for opening and securing doors.

### 14. Electronic Access Card Database

Information related to the electronic access card database is considered confidential, and only the key control coordinator and campus security will have access to view access card transaction history. All other requests for access card database information must be approved by the VCAS or the chancellor.