TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

No.1305 Rev.: 0

Policies and Procedures **Date: June 29, 2017**

Subject: Physical Key and Electronic Card Access

1. Purpose

An essential element of security is maintaining adequate access control to college facilities. This policy establishes a key control and electronic card access management plan to help protect the life, property, and security of Tidewater Community College employees, students, and visitors. It shall serve as the framework by which key and card access credentials will be managed, issued, duplicated, controlled, returned and replaced, and accounted for by responsible stakeholders.

2. Policy

Tidewater Community College controls access to college facilities by restricting keys and electronic card access to members of the college community based on an individual's core duties and responsibilities. College personnel are subject to corrective action for the unauthorized possession and use of keys and electronic cards and may be subject to prosecution under Code of Virginia §18.2-503 for the possession or duplication of certain keys. To effect this policy, TCC shall publish a Key Control and Electronic Card Access Management Plan which will delineate specific guidelines, responsibilities, and procedures.

3. Responsibilities

3.1. Chief Operating Officer for Facilities and Public Safety

The Chief Operating Officer for Facilities and Public Safety is responsible for providing executive direction and oversight of the College's Key Control and Electronic Card Access Management Plan. This includes the development and maintenance of procedures within their areas of responsibility to provide consistent practices between the key control system and the electronic card access system.

3.2. Director of Facilities Maintenance

The Director of Facilities Maintenance is responsible for managing and coordinating the College's physical key control program; authorizing the duplication of keys; collaborating with campus provosts and their designees to design the master, sub master, and change keys to individual rooms; ensuring the accountability of keys that are issued and returned; maintaining an accurate and complete inventory of keys and associated key codes; and collaborating with other stake holders that require keys to perform their duties. The Director of Facilities Maintenance shall collaborate with the Director of Public Safety to align key control and electronic card access procedures and practices.

3.3. Director of Public Safety

The Director of Public Safety is the Electronic Access Control Application Administrator. The Administrator is responsible for managing and coordinating the College's electronic card access program; collaborating with campus provosts and their designees to design the master, sub master, and individual room access groups; ensuring the accountability of card access privileges that are issued and removed; maintaining an accurate and complete database; and collaborating with other stakeholders that require electronic card access to perform their duties. The

Director of Public Safety shall collaborate with the Information Systems Electronic Access Software System Administrator and the Director of Facilities Management and Services to align electronic card access and key control procedures and practices.

3.4. Vice President for Workforce Solutions and Campus Provosts

The Vice President for Workforce Solutions and Campus Provosts, or their designees, are responsible for identifying Department and Campus Access Coordinators to collaborate with the Director of Facilities Management and Services and with the Director of Public Safety to assist in organizing the key control and electronic card system on each of their campuses, consistent with the Key Control and Electronic Access Control Management Plan.

3.5. Deans, Directors, and Supervisors

Deans, directors, and supervisors are responsible for identifying the type of key and electronic card access level their employees are authorized to possess consistent with the Key Control and Electronic Access Control Management Plan. Deans, directors, and supervisors are responsible for requesting keys through the Facilities Management Department, issuing the keys to employees, obtaining the keys back upon separation from employment or transfer, and documenting the transactions. Deans, directors, and supervisors are responsible for requesting electronic card access privileges through the Public Safety Department and for notifications to the Public Safety Department of changes in electronic access privileges.

3.6. Associate Vice President for Human Resources

The Associate Vice President for Human Resources or designee is responsible for entering new employee information into the college's database and notifying supervisors when new employees are officially employed so that supervisors may initiate the process to obtain keys, identification cards, and electronic access privileges. The Associate Vice President, or designee, is responsible for updating employee information for termination and transfer to ensure the return of keys that were issued and the removal of electronic access privileges.

3.7. ID Card Office

The ID Card Offices are responsible for issuing electronic access identification cards to all faculty, staff, authorized non-college personnel, and authorized students. Faculty and staff will be eligible to receive electronic access identification cards when their "info identification numbers" are entered into the access control database during their first week of employment. Authorized non-college personnel and students are eligible to receive electronic access identification cards upon approval by the Public Safety.

3.8. Vice President for Information Systems

The Vice President for Information Systems, or designee, is responsible for identifying an Electronic Access Software System Administrator to provide system administrative support for the electronic card access control software, and collaborating with the Department of Public Safety for the management of the

electronic card access system. The Office of Information Systems, the Facilities Department, and the Department of Public Safety, in collaboration, will facilitate the use of the TCC Intranet when aligning procedures for the authorization process to issue keys, grant electronic access privileges, return keys, remove electronic access, or transfer of employment to another location within the college.

3.9. Employees, Authorized Non-college Personnel, and Authorized Students

Each TCC employee, authorized non-college personnel, and authorized student has an individual responsibility to comply with the program elements and requirements established in the Key Control and Electronic Access Control Management Plan and may be subject to sanctions for failing to abide.

3.10. College Security Committee

The committee will monitor compliance with this policy and the Key Control and Electronic Access Control Management Plan across the college and recommend corrective actions to the Executive Director of Real Estate Development and COO of Facilities.

4. Rules and Standards

4.1. Possession of Keys and Electronic Access Cards

No person shall knowingly possess any key or electronic access card to the lock of any building, room, or other property owned by the college without receiving permission from an authorized college representative.

4.2. Duplication of Keys and Electronic Access Cards

No person shall knowingly duplicate, copy, or make a facsimile of any key or electronic access card to a lock, building, room, or other property owned by the college.

4.3. Reporting Lost or Damaged Keys and Electronic Access Cards

Lost and damaged keys or electronic access cards should be immediately reported to the supervisor and to the Department of Public Safety.

4.4. Responsibility for Lost or Damaged Keys and Electronic Access Cards

Charges may be assessed for lost or damaged keys and electronic access cards as specified in the Key Control and Electronic Access Control Management Plan.

5. Procedures

The college's Key Control and Electronic Card Access Management Plan shall provide procedures and processes to specify how keys and card access credentials will be managed, issued, duplicated, controlled, returned and replaced, and accounted for by responsible stake holders.

5.1. Key Control and Electronic Card Access Management Plan

Under the direction of the Executive Director of Real Estate and COO of Facilities, the Director of Public Safety and the Director of Facilities Management and

Services will develop and maintain the Key Control and Electronic Card Access Management Plan. The plan will be published on the college's website such that it is accessible to all members of the college community.

In developing and maintaining the plan, the Director of Public Safety and the Director of Facilities Management and Services shall ensure that its provisions, including assignments of responsibilities, are coordinated with the affected members of the President's Executive Staff and their respective management staff.

5.2. Key Control and Electronic Card Access Management Plan Contents

The plan will include specific procedures, assignment of responsibilities, and program guidelines. At a minimum, the plan will address/include:

- Key Control and Electronic Card Access Management Administration
  - Assignment of Responsibilities
  - Job Description Requirements
  - Managers' Performance Expectations
  - Process to authorize and issue keys for faculty and staff
  - Process to authorize and issue keys to non-college personnel and authorized students
  - Process to report and replace lost or damaged keys
  - Process to return keys due to termination or change of duties
  - Process to obtain a college electronic identification card
  - Process to obtain authorization for electronic access privileges for faculty and staff
  - Process to authorize and issue electronic access privileges to non-college personnel and authorized students
  - Process to report and replace lost or damaged electronic cards
  - Process to remove electronic access privileges due to termination or change of duties.
- College Security Committee
  - Annual Plan Review
- Key Control System Design
  - Master keys
  - Sub-master keys
  - Individual room (change) key
  - Key cut bitting
- Electronic Card Access System Design
  - Master all campus access groups
  - Sub-system campus access groups
  - Individual room access groups

- Key Pad and Combination Locks
  - Procedure for issuing codes and combinations
  - Procedures for changing codes and combinations
- Building and Room Access
  - Building hours of operation
  - Restricted access areas
  - Levels of authorized access
  - Emergency public safety access: Knox box fire access
- Human Resource Department Procedures for Key and Card Access
  - New hires
  - Transfers
  - Termination
- Standards and Rules
  - General rules and responsibilities
  - Fees for replacement and lost key and cards
  - Responsibilities of employees
  - Responsibilities of authorized non-college personnel
  - Responsibilities of authorized students
- Supervisory Procedures
  - New hires
  - Transfers
  - Replacement
  - Termination

6. Definitions

Authorized Non-college Personnel: Includes vendors, contractors, interns, tenants and municipal employees providing services, have lease agreements or work in conjunction with college staff and require access to areas that are secured by key or electronic access control.

Authorized Students: Includes work study or enrolled students assigned to work, study, or have access to areas that are secured by key or electronic access control.

Bitting: The number(s) that represent(s) the dimensions of the physical key cut(s) that are the actual cut(s) or combination of a key for use to unlock or lock a door.

Change Key: Lowest level key in a key system and opens a single door or doors that are cut to the same bitting.

Department and Campus Access Coordinator: Individuals assigned to coordinate with the Director of Facilities Management and Services and the Director of Public

Safety to help organize the key control and electronic card system for each of their respective campus locations.

Electronic Access Control: Access control using electronic or electromechanical devices to replace or supplement mechanical key access. Electronic access is administered through a computerized card access control system.

Electronic Access Control Application Administrator: Department of Public Safety employee who is responsible for the operation of the electronic card access system and overseeing the organization of the card reader devices, the grouping of access levels and the entering and deletion of access control authorizations.

Electronic Access Software System Administrator: Office of Information Systems employee who is responsible for maintenance of the electronic card access software.

Info Identification Number: Employee identification number.

Key Control: Any method or procedure which limits unauthorized acquisition of a key and/or controls distribution of authorized keys. A systematic organization of keys and key records.

Master Key or Card Access: Any combination of electronic card access or key access design that opens all doors on an existing campus location.

7. References

Code of Virginia § 18.2-503. Possession or duplication of certain keys:

http://law.lis.virginia.gov/vacode/title18.2/chapter12/section18.2-503/.

TCC Policy 1302 College Identification Cards:

https://web.tcc.edu/policies/1000/1302CollegeIdentificationCards.pdf.

8. Review Periodicity and Responsibility

The Executive Director of Real Estate and COO of Facilities shall review this policy at the anniversary of its approval and, if necessary, recommend revisions.

9. Effective Date and Approval

This policy is effective upon its approval by the College President on June 29, 2017.

Policy Approved:	Procedure Developed:
Edna V. Baehre-Kolovani, Ph.D. President	Matt Baumgarten COO for Facilities and Public Safety

10. Review and Revision History

This is the first version of this policy.