

Subject: Physical Key and Electronic Card Access Policy

1. Purpose	1
2. Policy.....	2
3. Responsibilities	2
3.1. Chief Operating Officer for Facilities & Public Safety	2
3.2. Director of Facilities Management.....	2
3.3. Director of Public Safety.....	2
3.4. Vice President for Workforce Solutions and Campus Provosts.....	3
3.5. Deans, Directors, and Supervisors.....	3
3.6. Associate Vice President for Human Resources.....	3
3.7. ID Card Office	3
3.8. Vice President for Information Systems	3
3.9. Employees, Authorized Non-college Personnel, and Authorized Students	4
3.10.College Security Committee.....	4
4. Procedures.....	4
4.1. Key Control and Electronic Card Access Management Plan	4
4.2. Key Control and Electronic Card Access Management Plan Contents	4
5. Definitions	5
6. References	5
7. Review Periodicity and Responsibility	6
8. Effective Date and Approval.....	6
9. Review and Revision History	6

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 control management plan to help protect the life, property, and security of Tidewater Community College facilities and the safety of faculty, staff, 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 stake holders.

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 the 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 & Public Safety

The Chief Operating Officer for Facilities & Public Safety (COO) is responsible for providing executive direction and management of the College's Key Control and Electronic Card Access Management Plan including developing and maintaining procedures within their areas of responsibility to provide consistent practices between the key control system and the electronic card access system. The COO shall appoint the College Security Committee comprised of members representing a cross-section of academic and administrative staff from each campus, off-campus facilities, and college's central administration to advise and review the development of the plan and its implementation.

3.2. Director of Facilities Management

The Director of Facilities Management is responsible for managing and coordinating the college's physical key control program, authorizes the duplication of keys, collaborating with campus provosts and their designees to design the master, sub master and change keys to individual rooms, to ensure the accountability of keys that are issued and returned, and to maintain an accurate and complete inventory of keys and associated key codes and to collaborate with other stake holders that require keys to perform their duties. The Director of Facilities Management 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 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, to ensure the accountability of card access privileges that are issued and removed, to maintain an accurate and complete data base, and to collaborate with other stake holders 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 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 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 Department of Public Safety and for notifications to the Department of Public Safety for 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 data base 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 for Human Resources or their 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, and to authorized non-college personnel and authorized students. Faculty and staff will be eligible to receive electronic access identification cards when their 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 Department of Public Safety.

3.8. Vice President for Information Systems

The Vice President for Information Systems or their designee is responsible for identifying an Electronic Access Software System Administrator to provide system administrative support for the electronic card access control software and collaborates with the Department of Public Safety for the management of the electronic card access system. The Office of Information Systems, the Department of Facilities Management and the Department of Public Safety, will work in collaboration to 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 College Security 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 Chief Operating Officer for Facilities & Public Safety.

4. 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.

4.1. Key Control and Electronic Card Access Management Plan

Under the direction of the Chief Operating Officer for Facilities & Public Safety, the Director of Public Safety and the Director of Facilities Management 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 shall insure that its provisions, including assignments of responsibilities, are coordinated with the affected members of the President's Cabinet and their respective management staff.

4.2. Key Control and Electronic Card Access Management Plan Contents

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

- Key Control and Electronic Card Access Management Administration
- College Security Committee
- Key Control System Design
- Electronic Card Access System Design
- Key Pad and Combination Locks
- Building and Room Access
- Human Resource Department Procedures for Key and Card Access

- Standards and Rules
- Supervisory Procedures

5. 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 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.

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

6. References

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

TCC Policy 1302 College Identification Cards

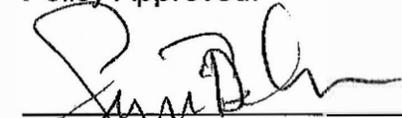
7. Review Periodicity and Responsibility

The Chief Operating Officer for Facilities & Public Safety shall review this policy at the anniversary of its approval and, if necessary, recommend revisions.

8. Effective Date and Approval

This policy is effective upon its approval by the College President on September 26, 2019.

Policy Approved:



Gregory Y. DeCinque, Ph.D.
Interim President

Procedure Developed:



Matthew J. Baumgarten
Chief Operating Officer for Facilities &
Public Safety

9. Review and Revision History

This is the first version of this policy.