Applicable Employee Classes:	**Reviewed Date:**	Approved by:
All Florida Tech Employees	4.30.2021	Dr. T. Dwayne McCay, President

POLICY: Access Control

PURPOSE

This policy defines responsibilities and outlines procedures for regulating access to Florida Institute of Technology assets and facilities. Balancing access with security is essential for both the safety and operation of the University. The *Department of Security* is responsible for overseeing this policy.

REPONSIBILITIES

Deans and Vice Presidents authorize access in respective areas, and:

- Provide the *Locksmith* with updates of access needed/no longer needed.
- Work with the *Locksmith* to conduct annual access audits.
- Collect hard keys from employees transferring to another department; employees expected to be on extended leave; and return the keys to the *Locksmith.*
- Collect all hard keys and ID Cards from resigned employees and return to the *Locksmith.*

Credential Holders (Key or Card holders) maintain possession of assigned credentials, and:

- Do not loan, transfer, duplicate, alter or dispose of hard keys or ID cards for any reason.
- Sign a Key Agreement before receipt of any keys.
- Retain all University-issued keys on a sealed security ring to be opened only by the *Locksmith or Department of Security*.
- Return hard keys and ID cards upon departure from the University to the *Locksmith*.

The *Locksmith* maintains control of all hard keys, mechanical locks, electronic access, ID cards and:

- Maintains inventory of all un-issued hard keys and associated locks/hardware.
- Maintains hard key database, associated locks/hardware and authorized *Key Holders*.
    - Information used to produce keys and locks is considered extremely confidential and will be accessible only to authorized *Locksmiths*.
- Reviews access requests in conjunction with the *Director of Security* to verify the requested level of access is appropriate, and that issuance would not create an unacceptable safety or security risk.
- Produces and issues approved hard keys and/or access cards.

- Annually conducts key audit with each department and/or Door Manager.
- Maintains inventory of ID cards and associated electronic access hardware.
- Maintains database of ID Card Key Holders, associated electronic access hardware and Door Managers.
- Maintains inventory of temporary/loaner keys for Facilities Operations Maintenance staff, vendors, and external contractors.

Campus Services issues, retrieves and maintains hard key inventory to residential facilities (for non-electronic locks only), and issues assigned resident hall and apartment card access to students; *Conference Services Bureau* maintains these responsibilities in regard to camp participants and special guests.

Information Technology supports the network infrastructure, software, and wiring to ensure the electronic access control system host remains online and operational.

Human Resources notifies the *Locksmith* of employee separations in a timely manner to confirm the departed employee's credentials have been returned/deactivated; exit paperwork is considered complete when hard keys and ID cards are received by the *Locksmith* and unassigned/deactivated in the employee record.

PROCEDURE

Requests for Access

A request for access is initiated by a *Dean or Vice President*, who submits an **Access Authorization and Request Form** on the *Department of Security* website. The *Locksmith* responds by identifying appropriate access requirements, verifies proper authorizations, and assigns access credentials. Requests not signed by a *Dean or Vice President* will not be processed.

Credentials may be temporarily issued to external contractors, vendors or tenants. Requests for temporary external contractor and vendor assignments shall include a contract agreement signed by the vendor including the date of expiration of these responsibilities to ensure timely return of hard keys, ID cards, combinations, or other access credentials. The *Locksmith* ensures the credentials are returned/deactivated at the end of the temporary assignment. Temporary credentials are not to leave campus and should be returned to the *Department of Security* each day. Outside parties responsible for the loss of issued hard keys must report the loss to the Department of Security immediately. This may result in re-keying costs to the outside parties.

On-Campus contractors (National, Barnes & Noble, ELS, etc..) and tenants will be assigned access credentials under the supervision of the *Department of Security* with approval from a *Dean or Vice President*.

All access credentials will be picked up and dropped off at the Department of Security; only the person to whom the keys are assigned may retrieve them.

Levels of Authorization

Hard Keys – Locksmith

- **Building Master Key:** Will operate all doors inside a single building; this is the highest-level key available for issue; additional authorization from the *Director of Security* and *Locksmith* is required.
- **Sub-Master Key:** Will operate a small group of doors/suite. Standard department and *Locksmith* approvals apply.
- **Operator Key:** Will typically operate a single door. Standard department and *Locksmith* approvals apply.
- **Restricted Area Keys:** High-security areas on file with the *Director of Security*; additional authorization from the *Director of Security* and *Locksmith* is required.

ID Card Access – Locksmith

- **Faculty & Staff Card Access:** Operates a specific assigned door or set of doors throughout campus on a pre-defined schedule. The *Locksmith* is responsible for all non-residential access authorizations and assignments.
- **Student ID Card Access:** Operates a specific assigned residence hall and an assigned apartment. The permissions are issued to student residents at assigned residence halls and assigned apartments. *Campus Services* issues assigned residence hall and apartment access to students.
- **Restricted Areas:** High-security areas on file with the *Director of Security* require authorization from a *Vice President*, the *Director of Security*, and the *Locksmith*.

GENERAL INFORMATION

Missing keys and ID cards must be reported immediately to the Department of Security. The *Locksmith and Director of Security* will then determine the extent of the potential breach. Missing hard keys usually result in re-keying of all affected locks, the cost of which will be borne by the department by which the key was authorized to be issued. Missing ID cards are deactivated and reassigned as needed. Students must report lost or stolen keys to *Campus Services* immediately and can obtain a replacement key upon payment of a $75 per key fee, or $25 fee per lost card. There is no charge for broken keys or cards as long as all pieces are returned to the *Locksmith*.

Installing personal locks in any University facility is prohibited, excluding personal lockers and similar storage. Furthermore, no alternate configurations or modifications can be made to any locking or keying system unless done so by the *Locksmith*.

Many doors are intended to be locked at all times and must never be propped open nor their locking mechanisms tampered with in any manner.

Spaces specifically designated as mechanical or electrical rooms, custodial storage, or telecommunications rooms are restricted for access by maintenance personnel only.

Keys are never issued for electronic locks equipped with hard key override. The *Department of Security* and *Locksmith* will be the only entities on campus authorized to possess the electronic override key. In the event an electronic lock experiences a total failure that cannot be resolved quickly, temporary cores may be installed for continued operation of the lock via a temporary hard key until it is repaired. This occurs rarely, and only with approval from the *Director of Security.*

Emergency keying may be implemented by the Director of Security under certain conditions which require **all** access in a given area be removed from **all** persons to ensure complete and total safety. In the event emergency keying is initiated, only the Director of Security can designate those receiving temporary emergency access credentials.

Construction keying will be utilized for new construction and capital projects only (buildings not yet under University occupancy). Construction locks are not part of the University master key system and are intended for contractors use only. In-house projects and smaller scale renovations will maintain their keying in the University master key system, assuming it does not create a safety or security concern to the occupant(s), and locks will only be changed in the event a key is not returned upon completion of the job.

Keys are never to be stored on campus unless inside a secure container approved and registered with the *Locksmith*. Any department having such a container registered must also designate someone as the responsible party for the secure container and its contents.

At no point can any member of the campus community be assigned multiple credentials providing access to the same space(s).

Keys remain the property of the University at all times and must be surrendered upon request by the *Department of Security or Locksmith*.