

SUBJECT: Facilities and Safety Employee Electronic Access to UCF Buildings	Effective Date: 4/19/2013	Procedure Number: FS 2013 FS0008	
	Supersedes:	Page 1	Of 2
	Responsible Authority: Associate Vice President, Administration and Finance (Facilities and Safety)		

APPLICABILITY/ACCOUNTABILITY:

This procedure applies to all A&P, USPS, and, where applicable, OPS employees within the Facilities & Safety section of Administration & Finance (Facilities & Safety, Environmental Health & Safety, Facilities Operations, Facilities Planning, Landscape & Natural Resources, Office of Emergency Management, Resource Management, Sustainability & Energy Management, and University Police).

PROCEDURE STATEMENT:

Facilities & Safety personnel will be given access to university buildings and controlled areas to perform their job functions. Electronic access card rights are issued for entry into university buildings for the purpose of conducting university business only. The holder of any access card assumes the responsibility for the proper use and safekeeping of that card, including reporting the card lost, stolen, or inoperable. Supervisors requesting electronic card access for their employees must use the Card Access Authorization Form or Key Request Form to receive appropriate approval.

PROCEDURE:

This procedure outlines the process for obtaining electronic access to Building 16A, as well as electronic access to buildings using the UCF ID card, and proximity cards.

Building 16A

- Facilities & Safety employees may obtain electronic access to Building 16A. The employee's supervisor will complete and sign the Card Access Authorization Form, noting the days, times, and entrances to which the employee is allowed access. The supervisor or the employee will submit the request form to the Card Access Administrator, accompanied by a photocopy of the employee's UCF card ID. The Access Card Administrator will review and process the request, or contact the supervisor, as needed, for additional information. Note: any requests for extended hours of access outside of the employee's normal work shift, including requests for 24/7 access, must be signed by the Assistant Vice President, Facilities.
- If a UCF card is lost or stolen, the employee will obtain another card from the UCF Card Office. A photocopy of the new card must be submitted to the Access Card Administrator to update access on the new card, and terminate access on the old card.

- If a card is inoperable, the employee must contact F&S HR/Payroll to obtain a letter to be given to the UCF Card Office to replace the card. The employee must exchange the old card for the new card, maintaining the same UCF ID card number.

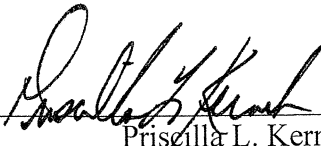
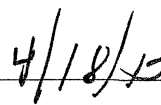
Suspension, Revocation, and Limitation of Electronic Access:

- If an employee's job function changes, a review of electronic access should be completed by the applicable director. The director will notify the locksmith to limit access if necessary.
- Upon suspension or disciplinary action, F&S HR/Personnel will notify the Access Card Administrator to suspend all access on the employee's cards.
- Upon termination, F&S HR/Personnel will notify the Access Card Administrator to revoke all access on the employee's cards.

Access to Buildings with Proximity Access Control:

- Employees requiring access must fill out a Key Request Form, obtain their director's approval, and submit the Key Request Form to the Associate Vice President of Administration and Finance (Facilities & Safety) (AVP) for approval.
- The AVP approves or disapproves, and forwards the request back to the director.
- Upon approval, the director instructs the employee to go to the Locksmith's Shop and show the signed Key Request Form to obtain a blank proximity card.
- The employee will go to F&S HR/Payroll to have his or her picture taken and added to the proximity card.
- The employee will take the Key Request Form and the proximity card or his or her UCF ID card to the Locksmith for processing and granting of requested access.
- The Locksmith will keep the Key Request Form, and record the access granted in the master database for Open Options.
- Employees must report lost or stolen cards to their supervisor, so that the access can be terminated, and another card issued.

Note: A proximity card is considered a GGM, and should always be protected and kept in a secure location. The only person authorized to use a proximity card is the employee to whom it was issued. In the event that proximity card is lost, stolen, or misplaced, the employee must contact his or her supervisor immediately. As with lost or stolen GGMs, disciplinary action may be taken for loss or theft of a proximity card.

Approved By:	Date Approved:
 _____ Priscilla L. Kernek Associate Vice President Administration and Finance Facilities and Safety	 _____