I. PURPOSE & INTENT

The purpose and intent of this Policy is to set forth procedures to provide for the security of Tampa Campus buildings, facilities, personnel and property, insofar as electronic building access, key control, and rekeying are concerned and, to establish a program of accountability and responsibility for control of access, and secure key control. The responsibility for building access of regional campuses or separately accredited institutions is not covered by this Policy and has been delegated to the Campus Executive Officer, Regional Chancellor or designee for each of these areas.

II. STATEMENT OF POLICY

A. The President of the USF System is the accountable officer for all USF System property. The Vice President for Administrative Services, Tampa Campus, is delegated the responsibility to ensure the safety and security of persons and property on the Tampa Campus against loss through vandalism, theft, misuse or other criminal activity within buildings and facilities on the Tampa Campus. Other than during normal working hours, or other than during officially scheduled events, all academic and administrative buildings, as logistically and physically possible, shall be locked in order to maintain the security of buildings, users, and contents.
B. Access to buildings, by key or other means, is granted for entry to buildings and facilities for the purpose of conducting official business only.

C. Tampa Campus office buildings shall be secured after normal working hours and classroom buildings after scheduled class hours. Faculty and staff who have not been granted access by the appropriate authority, by key or other means, will be denied access by University Police until such authorization has been afforded. Limited access to building exterior doors may be permitted if approved by their immediate Vice President, Dean, Director or Chairperson.

III. DEFINITION OF TERMS

A. As used in this Policy, the term "key" also refers to any device or system which locks or otherwise secures a Tampa Campus facility and contents. This includes, but is not limited to, electronic card access, combinations and codes for alarm systems, electronic and mechanical locking devices, etc. in which the same procedures for keys may apply.

B. For purpose of this Policy “department head” shall be defined as Vice President, Dean, Director, Chairperson, or designee

IV. INDIVIDUAL ACCESS HOLDER RESPONSIBILITIES

A person possessing a key or access card is responsible for the security and proper use as follows:

A. Safeguarding and using the key or access card to access assigned areas for official business only.

B. Not loaning a key or access card to any other person.

C. Preventing the duplication of any key or access card assigned to them.

D. Locking doors, files, cabinets, etc. for which a key or access card is issued, as appropriate.

E. Reporting to the Tampa Campus University Police any condition he/she may observe which may jeopardize property or personnel.
F. Assuming responsibility for the conduct of any person the holder allows to enter a building or facility, as the result of his or her possession of a key.

G. Immediately notifying the Tampa Campus University Police and the department head when a key or access card is lost or stolen, when the key is a master key or when the key/card opens sensitive areas such as cashier's office, pharmacy, lab, etc., or if the key/card provides access to sensitive materials.

H. Returning the keys to the KEY SHOP when no longer needed.

I. Agreeing that he/she understands his/her personnel record may not be cleared when terminating, transferring, or going on leave until his/her key record is cleared.

V. PHYSICAL PLANT RESPONSIBILITIES

Physical Plant will perform an annual audit of the list of personnel who are authorized to provide and remove access to others.

VI. COLLEGE, DIVISION, DEPARTMENT RESPONSIBILITY

The various Colleges, Divisions, Departments that provide and remove access to other are responsible as follows:

A. A Dean, VP, Director (or designee) will identify “Authorizer(s)” who will be provided the authority to approve and remove access for other building occupants, and will communicate this Authorizer(s) to Physical Plant in a manner Physical Plant deems appropriate.

B. The Authorizer will only provide access for needed business purposes.

C. The Authorizer will remove access as soon as possible when the assigned access is not required or as soon as the person with the assigned access in no longer with the University.

D. The College, Division, Department will perform at least an annual audit of the access provided to others.

E. The Dean, VP, Director (or designee) will inform Physical Plant Division in a timely manner when a previously designated Authorizer no longer requires Authorizer privileges as part of their responsibilities, or when that employee separates from the University, or transfers from the Dean, VP, Director or designee's area.
F. Authorizers must be identified/coded in the USF Identity Management System as a University employee or as a tracked affiliate.

VII. PENALTIES FOR VIOLATION OF POLICY

A. Negligence in the loss or use of a key or access card is a serious matter. Violations of this Policy, through negligent behavior on the part of any staff or faculty member, shall result in appropriate disciplinary action and/or a $50 pay setoff to be used to defray costs of rekeying in case of a lost key. Illegal use of a key or access card may lead to criminal investigation and eventual criminal charges.

B. Keys assigned to faculty or staff which are not returned may lead to a $50 pay setoff to be used to defray rekeying costs.

*Current Responsible Office: Administrative Services

*Refer to the appropriate Responsible Office website for a current name of the Vice President or other Responsible Officer.