SECTION: Information Technology **Policy 04.06.18**
AREA: Information Security

SUBJECT: Physical Access Policy

I. INTRODUCTION

Technical support staff, security administrators, system administrators, and others may have information resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to information resources and technology facilities is extremely important to an overall security program.

II. PURPOSE

The purpose of the Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to information resource and technology facilities. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

III. SCOPE

The University Physical Access Policy applies to all individuals within the University enterprise who are responsible for the installation and support of information resources and technology, individuals charged with information resources and technology security, and data owners.

IV. POLICY

A. All physical security systems must comply with applicable regulations including, but not limited to, building and fire prevention codes.

B. Physical access to information resources and technology restricted facilities must be documented and managed.

C. All information resource and technology facilities must be physically protected in proportion to the criticality or importance of their function at the University.

D. Access to information resources facilities must be granted only to University support personnel and contractors whose job responsibilities require access to that facility.

E. The process for granting card and/or key access to information resources and technology

facilities must include the approval of the person responsible for the facility.

F. Each individual who is granted access rights to an information resources and technology facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

G. Requests for access must come from the applicable University data/system owner.

H. Access cards and/or keys must not be shared or loaned to others.

I. Access cards and/or keys that are no longer required must be returned to the person responsible for the information resources and technology facility. Cards shall not be reallocated to another individual bypassing the return process.

J. Lost or stolen access cards and/or keys must be reported to the person responsible for the information resources and technology facility.

K. Cards and/or keys must not have identifying information other than a return mail address.

L. All information resources and technology facilities that allow access to visitors will track visitor access with a sign in/out log.

M. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.

N. Card access records and visitor logs for information resources and technology facilities must be kept for routine review based upon the criticality of the information resources and technology being protected.

O. The person responsible for the information resources and technology facility must remove the card and/or key access rights of individuals who change roles within the University or are separated from their relationship with the University

P. Visitors must be escorted into card access controlled areas of information resources and technology facilities.

Q. The person responsible for the information resources and technology facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

R. The person responsible for the information resources and technology facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

S. Signage for restricted access rooms and locations must be practical although minimal

discernible evidence of the importance of the location should be displayed.

V. DISCIPLINARY ACTION

Violation of this policy may result in immediate Disciplinary Action pursuant to University policy (MAPP 02.05.03 – Discipline and Termination Policy).

VI. APPLICABLE TSU SECURITY POLICY STANDARDS

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22). Applicable security standards include, but are not limited to:

- Security Standard 5
- Security Standard 8
- Security Standard 9
- Security Standard 16
- Security Standard 19

VII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

Review: Every year, on or before September 1

VIII. APPROVAL

Vice President of Finance

President

2/18/11

Effective Date