SECTION: Information Technology **Policy 04.06.19**
AREA: Information Security

SUBJECT: Portable Computing Policy

I. INTRODUCTION

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to individuals or groups who use the devices.

II. PURPOSE & SCOPE

The purpose of the Portable Computing Policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of the network and University information. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The Portable Computing Policy applies equally to all individuals who utilize portable computing devices and access University information resources and technology.

III. POLICY

A. Only University approved portable computing devices may be used to access University information resources and technology.

B. Portable computing devices must be password protected.

C. University data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive University data must be encrypted using approved encryption techniques.

D. University data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.

E. All remote access (dial in services) to the University must be either through an approved modem pool or via an Internet Service Provider (ISP).

F. Non-University computer systems that require network connectivity must conform to University standards and must be approved in writing by the University Information Security Officer.

G. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

IV. DISCIPLINARY ACTION

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

V. 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 1
- Security Standard 3
- Security Standard 5
- Security Standard 7
- Security Standard 12
- Security Standard 20

VI. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

Review: Every year, on or before September 1

VII. APPROVAL

Vice President of Finance

President

2/18/11
Effective Date