Administrative Guideline 1115

ADMINISTRATIVE GUIDELINE TYPE: Information Technology
ADMINISTRATIVE GUIDELINE TITLE: Employee Guidelines for Securing Mobile Technologies

DEPARTMENT RESPONSIBLE: Information Technology
GUIDELINE STATEMENT OF PURPOSE: Employee Guidelines for Securing Mobile Technologies

1. Statement of Purpose

Mobile technologies (laptops, USB drives, mobile drives, PDA's, etc.) offer staff the ability to be more productive while on the move. However, mobile technologies are a significant security risk to Southeastern Community College (SCC) employees, students and community members. Mobile technologies increase our risk of confidential data theft and unauthorized access to our systems.
SCC employees must be aware and take measures to protect confidential data and systems both within and outside of our work environment. The following guidelines were developed to help ensure all measures are taken to protect the college and the people we serve.

2. Protecting Mobile Devices

In order to qualify for access to our corporate network, the laptop must meet the following conditions:

A. All SCC mobile devices (laptops, USB drives, CD's, DVD's, etc.) that store electronic files with 'confidential information' must be encrypted to prevent unauthorized access if lost or stolen. All employees should contact the Information Technology Services department to ensure that these types of files are encrypted.

B. All SCC mobile computers must have antivirus software installed. ITS will install and enforce this guideline.

C. All SCC mobile computers must install and activate a personal firewall.