ROGERS STATE UNIVERSITY

Mobile Device and Storage Media Security Policy

Approved by:

Date Approved: 3-24-09

Rogers State University
Mobile Device and Storage Media Security Policy

I. Purpose

Because of the ease of transport of laptop computers and other mobile devices, there is a higher rate of theft for these devices. This policy is designed to help prevent such thefts, as well as protect any data stored on these devices.

II. Scope

This policy applies to all laptops, mobile devices, and storage media that are owned by Rogers State University and/or are used for conducting business for Rogers State University.

III. Policy

Physical Security

- Laptop computers and other mobile devices should be secured with a locking cable or other securing device whenever possible to deter theft.
- Laptop computer stewards are responsible for taking reasonable and prudent measures to ensure the physical security of the equipment. When left unattended in an unsecured area, the equipment must be physically secured using a locking mechanism. While in transit or stored offsite, stewards must take reasonable and prudent measures to ensure security of equipment against loss or theft

Technical Security

Full Disk Encryption (FDE)

- University faculty and staff are required to encrypt any mobile device that stores Category III Protected Data (See Data Classification Policy) using whole or full disk encryption (FDE). In cognizance of FDE, storage and use of sensitive, confidential or proprietary data should be considered temporary and transient in nature.

Authentication

- Authentication with strong passwords is required on all laptop devices. A strong password is one that is not obvious or easy to guess. Whenever possible, your password should be 8-32 characters long and include a combination of upper and lowercase letters, numbers and special characters.

Sensitive or Proprietary Data

- It is strongly encouraged that, even when using encryption technologies, laptop computer stewards not store confidential or sensitive data on laptop computers or other mobile devices unless absolutely necessary to conduct University-related business.

Use of Non University Laptops

- Employees using personally owned laptops for University business are personally responsible for meeting all the security requirements of Rogers State University.