Siena College Laptop and Portable Electronic Devices Security Policy

I Purpose:

Siena College is concerned with keeping data secure. There are special problems with data kept on laptop computer; if the laptop is stolen or lost, sensitive information can get into the hands of outsiders. Siena is required by law to notify anyone whose personal information may have been compromised. In order to avoid that, there are some practices that are needed.

Laptop computers as well as all portable electronic devices capable of storing data provide important functionality, enabling Siena College faculty and staff to have their computing resource at hand in meetings/classes, and those who travel on college business or work off campus to be maximally functional and productive. Unfortunately, the college realizes the possibility of the loss of laptops and other storage medium due to theft. A potential loss of a laptop (including data stored in memory, on disks or memory sticks) to the college is substantial and represents losses in dollars, productivity, and the potential for an information security breach. This policy addresses the actions that must be taken to safeguard information and to minimize the risk of theft of college owned laptops along with the associated impact on the college.

II Scope:

This policy applies to all faculty, staff, and students who use a Siena College owned laptop or any device or storage medium that contains college data. These individuals are hereinafter referred to as "caretakers." Each caretaker of a college-owned laptop is responsible for the security of that laptop, as well as all stored data, regardless of whether the laptop is used in the office, at one's place of residence, or in any other location such as a hotel, conference room, car or airport. Laptop users must abide by the rules for storage of information as documented in this policy similarly to any computer devices. Laptop computers and portable electronic devices such as Smart Phones and Tablets, require extra security in case they are lost or stolen.

III Policy Statement:

Only data necessary for work is to be downloaded onto the computer, and confidential information is never to be kept on portable computer devices. It is strongly urged that users encrypt any sensitive files they have on their devices, and to use password protection on the device.

A. Required Computer Security Training, Encryption of Data, and Signed Acknowledgement Form

Prior to a caretaker being issued possession of a college-owned laptop, s/he will complete a Siena College ITS Laptop Security Training class (currently online using Blackboard) that among other things will teach why it is necessary to secure and encrypt data along with the steps involved. At the conclusion of the seminar each attendee will receive a copy of the most recent Laptop and Computer Use Policies, and read, sign, and date an Acknowledgement Form to be kept on file indicating an agreement to abide by all Siena College Laptop, Computing Use and data security policies. Such acknowledgement will be made on an annual basis.

B. Laptops in Campus Offices

A caretaker of a college-owned laptop will be provided a security cable to attach the laptop to an immovable object (typically a desk) in the caretaker's campus office. ITS will issue the cable, provide advice and installation assistance. Although use of the cable is encouraged, the user is left to decide when to actually employ it. If a laptop caretaker is going to be out of the office for one day or more, s/he is expected to store the laptop and storage medium out of sight in a locked cabinet.

C. Laptops Outside of Campus Offices

When a caretaker takes the laptop out of his/her office, s/he is expected to keep the laptop in hand or sight, or in a secure and locked location, at all times. An engaged laptop lock is encouraged even during use.

D. Reporting a Theft

If a college-owned laptop or any data is stolen or missing, its caretaker is expected to immediately file a report with the Siena College Safety and Security Office.

IV Governance:

This policy will be updated by the Department of ITS. It will be approved by the CIO and President's Cabinet.

V Exceptions:

Exceptions can be granted in limited circumstances by the CIO based upon the needs of the College and upon the requestor's written justification, which has been reviewed and approved by the College's Risk Officer.

VI Revision History:

Date	Revision #	Modification	Approved Date
2/08/07	1.0	Cabinet Approval	2/08/07