Laptop Full Disk Encryption Standard
Syracuse University – Information Technology and Services
Information Security Standard – S0100

1.0 Scope

- All Laptop computers owned by Syracuse University
- All non-SU owned laptop computers used by SU faculty/staff that store SU data classified as "confidential" or "enterprise".

2.0 Purpose

The purpose of this standard is to protect Syracuse University data via the encryption of all data that resides on a laptop computer's hard drive. Enacting this standard protects SU from costly breach notification requirements since encrypted data is not considered compromised in the event of a laptop computer's loss or theft.

3.0 Standard

3.1 SU Owned Laptops:

All laptop computers owned by Syracuse University that are running Windows Vista or Windows 7 are required to employ the full disk encryption solution "CheckPoint FDE" currently funded by ITS and laptops owned by Syracuse University that are running Windows 8 and higher are required to employ the full disk encryption solution "BitLocker" provided as part of the operating system as described in the ITS procedures for Full Disk Encryption (see section 5.0 references).

Systems running Mac OS X 10.6 (Snow Leopard) are required to employ the full disk encryption solution "CheckPoint FDE" currently funded by ITS and laptops owned by Syracuse University that are running Mac OS X 10.7 (Lion) or higher are required to employ the full disk encryption solution "File Vault 2" provided as part of the operating system as described in the ITS procedures for Full Disk Encryption (see section 5.0 references).

All Requests for exceptions to this standard should be handled as per Section 4.0 "Exceptions" below.

3.2 Non SU Owned Laptops

Laptop computers not owned by Syracuse University **MAY NOT** store University data that has been classified by the ***Syracuse University Information Security Standard*** (see Section 5.0 references) as "confidential" or "enterprise". Therefore, encryption is not funded for non-SU owned laptops.

Note: See Section 4.3 below for exceptions concerning adjunct faculty, teaching assistants and graduate assistants keeping limited amounts of student data on their personally owned laptops.

4.0 Exceptions

4.1 SU Owned Laptops that will not store confidential or enterprise data

Any individual seeking an exception to this standard, and who will not store confidential or enterprise data on the laptop must complete and sign the ***Full Disk Encryption Exception Form*** (see Section 5.0 references). This form requires the signature of the end user and the IT Director of the unit that owns the laptop for which the exception is being sought. The exception states that the end user of the laptop as well as the host unit accept the responsibility to perform due diligence in ensuring that no confidential or enterprise data will be stored on the laptop in question.

4.2 SU Owned Laptops that will store confidential or enterprise data

Exceptions for laptops that **will** store confidential or enterprise data can only be granted by the Information Security Officer (see contact information below). The end user of the laptop as well as their local IT support staff must schedule a meeting with Information Security Officer to discuss the need for the exception and possible alternative protections.

4.3 Personally owned laptops for adjunct faculty, teaching assistants and graduate assistants

Since Syracuse University does not fund the purchase of laptop computers for its adjunct faculty, teaching assistants or graduate assistants, these individuals may store limited confidential or enterprise data pertaining to classes they are currently teaching on their personally owned laptop, (I.e. class roster and unofficial grades). This data should be limited to only what is needed to teach their classes, and should be removed from the system as soon as it is no longer required. This is a blanket exception and requires no action on the part of the unit or the laptop owner.

5.0 Referred Documents, Web Pages and Contact Information

Item	Location/Info
Procedure: *Full Disk Encryption (FDE) Setup – Windows On-Domain*	https://answers.syr.edu/display/infosec101/Full+Disk+Encryption+(FDE)+Setup+-+Windows+On-Domain (requires logon to answers.syr.edu)
Procedure: *Full Disk Encryption (FDE) Setup – Windows Off-Domain*	https://answers.syr.edu/display/infosec101/Full+Disk+Encryption+(FDE)+Setup+-+Windows+Off-Domain (requires logon to answers.syr.edu)
Procedure: *Full Disk Encryption (FDE) Setup – Mac OS X*	https://answers.syr.edu/display/infosec101/Full+Disk+Encryption+(FDE)+Setup+-+Mac+OS+X (requires logon to answers.syr.edu)
Procedure: *Full Disk Encryption (FDE) Setup – Using FileVault for MAC OX X (10.7 or later)*	https://answers.syr.edu/display/infosec101/FDE+for+MAC+OS+X+Lion+and+Mountain+Lion
Standard: *Syracuse University Information Security Standard*	http://its.syr.edu/security/standards/ITSecurity-standard.pdf
Form: *Full Disk Encryption Exception Form*	http://its.syr.edu/security/standards/fde-exception-form.pdf

Contact: Information Security Officer	Christopher Croad ccroad@syr.edu

Document Info

Version:	1.04
Effective Date:	March 1st, 2011
Date of Last Review	Sep 5th, 2015
Date of Next Mandatory Review	March 15st 2017