EMORY
LIBRARIES &
INFORMATION
TECHNOLOGY

Policy 5.12 – Disk Encryption Policy

Implementation Guide

1. Purpose

This implementation guide is provided as a reference to help members of the Emory community implement the updated requirements of Policy 5.12 – Disk Encryption Policy (http://policies.emory.edu/5.12) Please contact LITS Information Security for any questions related to this guide, or to the policy.

2. Frequently Asked Questions

A. How do I know if I have a portable computing device?

A **portable computing device** can be further defined as any device that is readily portable (small and designed for mobility), running an end-user class operating system (Windows or Mac OS X) and has self-contained input, output, and processing capabilities, such as a keyboard, display, and CPU. Examples include, but are not limited to:

- Laptops (even when docked using a docking station)
- Netbooks
- Tablet PCs

Note: Devices such as smartphones and tablets running Mobile operating systems (iOS, Android, Windows Phone OS, Blackberry OS) are covered under Emory's smart device security policy, 5.14.

B. How do I know if I have a desktop computing device?

A **desktop computing device** can be further defined as any device that is not readily portable (not designed for mobility), running an end-user class operating system (Windows or Mac OS X) and does not have self-contained input, output, and processing capabilities, such as a keyboard, display, and CPU. Examples include, but are not limited to:

- Desktop PC
- iMac
- Mac Mini
- All-in-one PC
- Small form factor (SFF) and ultra small form factor (USFF) PC

C. How do I know if my device meets the definition of "personally owned"?

Personally owned desktop and portable devices can be further defined as those whose primary uses are personal and not business in nature, and generally are not supported by Emory IT personnel. Examples include, but are not limited to:

- A device purchased with someone's personal funds, even when used for Emory business
- A device purchased with Emory's funds, professional development funds, or grant funds for use at home, and is not supported by IT personnel
- A device given to someone by Emory when they depart the institution

Storing Emory confidential or restricted data on these devices is expressly prohibited by policy 5.12.

D. Does my Smart Phone or Tablet have to be encrypted?

Devices such as smartphones and tablets running mobile operating systems (iOS, Android, Windows Phone OS, Blackberry OS) are covered under Emory's smart device security policy, 5.14. These devices are out of scope for this policy.

E. Do public or shared use portable computers require encryption?

If the following statements are **all true**, then the device may be exempted from the encryption requirement:

- The device is intended for shared or public use. Examples include: Conference rooms, kiosks, and computer labs.
- Emory Restricted or Confidential data are not stored on the device
- The device is physically secured via a cable or security plate
- The device is intended to be stationary and is not moved or taken to other physical locations

F. Do loaner laptops require encryption?

Yes. The only exception is in the event that the laptop will be brought to a country with export control restrictions, or restrictions on encrypted devices coming into the country. In these cases restricted or confidential data must not be stored on the device.

For all other uses, loaner laptops do require encryption. In this scenario boot passwords will need to be given to each user that checks the device out. It is **extremely important** that the password never be stored in a written form on or with the laptop.

G. Do laptops running Linux require encryption?

Laptops running the Linux operating systems should be encrypted as well. Please see http://it.emory.edu/security/disk_encryption.html for guidance on encrypting Linux systems.

H. Do Chromebooks require encryption?

Chromebooks run a modified version of the Linux operating system, and are outside of the scope of this policy. However, Chromebooks automatically encrypt user data by default and as such would meet the requirements.

I. Do portable computers attached to lab equipment require encryption?

Every effort should be made to encrypt these devices as well. Some circumstances that allow exceptions are:

- The device is vendor supported and encryption is not permissible by the vendor. The vendor must explicitly state this restriction.
- The device is under federal or state regulatory control, and the governing agency explicitly forbids encryption.
- The device's OS does not support encryption and upgrading is not an option because of device compatibility.

In the event that any of the above conditions are true, the device must be physically secured using a security cable or plate, and confidential or restricted data may not be stored on it past the point of collection.

J. Should backups of encrypted systems be encrypted as well?

Yes. Backups of encrypted systems that are stored on physical media (external hard drive, flash drive, etc.) must utilize disk encryption as well. If data is backed up to a file server, CrashPlan, or Emory Box, then this does not apply. Both FileVault and MBAM/BitLocker support encrypting external media. Flash drives that have built-in hardware encryption capabilities are also permissible and very useful in cases where cross platform support is required. For a list of approved models, please visit: http://it.emory.edu/security/disk_encryption.html.

K. Does my desktop computer need to be encrypted?

If your desktop contains 500 or more records of restricted data, as defined by the policy, yes. However, encryption is recommended on any desktop system that stores any restricted data. Encryption is also recommended on any desktop storing more than 500 or more records of confidential data, as defined by the policy.