# Policy 5.12
# Disk Encryption Policy

**Responsible Official:** VP for Information Technology & CIO

**Administering Division/Department:** Office of Information Technology

**Effective Date:** August 07, 2009

**Last Revision:** August 24, 2009

**Policy Sections:**



**Overview**

This policy establishes requirements and guidelines for the use of disk encryption technologies on Emory computing devices to protect the confidentiality of sensitive information. This policy is effective immediately for new systems. Existing systems have 6 months from the effective date of this policy to fully implement the requirements, unless otherwise noted.

**Applicability**

This policy applies to all Emory-owned, and personally-owned, desktop and portable computing devices storing Emory-managed data.

**Policy Details**

1. Required and recommended situations for *portable computing device encryption*
    a. All *portable computing devices* containing *restricted data* must employ *whole disk encryption*, as defined in this policy, to protect this data. Conversely, any *portable computing devices* not employing *whole disk encryption* as defined in this policy must not store *restricted data*.
    b. All *portable computing devices* containing *confidential data* should employ *encryption*, as defined in this policy, to protect this data.
    c. Use of *whole disk encryption* is recommended for all *portable computing devices*.
2. Required and recommended situations for *desktop computing device encryption*
    a. All *desktop computing devices* containing more than 500 *restricted* data records must employ *whole disk encryption*, as defined in this policy, to protect this data. Conversely, any *desktop computing devices* not employing *whole disk encryption* as defined in this policy must not store more than 500 *restricted* data records.
    b. All *desktop computing devices* containing between 1 and 500 *restricted* data records should employ *whole disk encryption*, as defined in this policy, to protect this data.
    c. All *desktop computing devices* containing more than 500 *confidential* data records should employ *whole disk encryption*, as defined in this policy, to protect this data.
3. Transient data exception
    a. *Portable computing devices* and *desktop computing devices* that contain *confidential* or *restricted* information solely in *transient data* files (i.e. files that do not remain on the computing device after a system power down or reboot) are not required to employ *whole disk encryption* to protect the information. However, whole disk encryption is still recommended in these situations.
4. Encryption implementation standard
    a. Only *whole disk encryption* solutions approved by the Office of the Chief Information Security Officer may be utilized to satisfy the requirements of this policy.
    b. The entire disk, or all user-writable local disk volumes, will be encrypted.

c. The *whole disk encryption* solution will centrally manage whole disk encryption client software for all systems, including encryption format, key management, and logging.
d. Emory will centrally maintain copies of encryption keys and encryption audit logs.
e. Emory retains the right to decrypt data using the centrally maintained key as required, using the employee data access approval process.

5. Deployment responsibilities
    a. It is the responsibility of the IT director in each organization to ensure that systems requiring encryption are identified, and that encryption is properly deployed on these systems.
6. End user responsibilities
    a. Users must report any known, unencrypted *restricted data* on *portable computing devices* to their local IT support staff and request assistance in removing the data or acquiring encryption software.
    b. Users must not attempt to disable, remove, or otherwise tamper with the encryption software.

**Definitions**

**Encryption:** A process by which data is transformed into a format that renders it unreadable without access to the encryption key and knowledge of the process used.

**Encryption key**: A password, file or piece of hardware that is required to encrypt and decrypt information – essentially "locking" and "unlocking" the information.

**Desktop computing device**: Any end user class computing device that is not readily portable and is capable of processing and storing Emory-managed electronic data . Examples: desktop computer, shared lab workstation, computer kiosk. Server class computers are not included in this definition.

**Portable computing device**: Any readily portable computing device capable of processing and storing Emory-managed electronic data. Examples: laptop computer, smart phone, personal digital assistant (PDA). ***Note: For purposes of this policy the portable computing devices considered in scope are limited to laptops and netbooks running Windows or OS X operating systems.***

**Portable data-storage device**: Any readily portable device or storage medium capable of storing Emory-managed electronic data. Examples: laptop computer, smart phone, personal digital assistant (PDA), USB drive, CD-R or DVD-R.

**Transient Data:** Data of any classification that may temporarily exist on a computing or data storage device for a limited amount of time (e.g. print spool files, website content cached by the browser, temporary files created while editing documents), but does not persist beyond a system power off or reboot.

**Whole Disk Encryption:** Encryption process in which the entire hard disk (or storage device) is encrypted thereby protecting all the data on the storage device.

**Data Classification Definitions:**

**Public data**: Any information that is intended to be read by the general public. Examples: the content of a publicly accessible website, the Emory University course catalog, the schedule for performance events, student information classified as "directory data"

**Internal data**: Any information that should only be read by, and distributed to, faculty, staff, and students of Emory. Examples: memos from campus administration to employees, general work documents that are neither intended to be public, nor contain confidential or restricted data (see definitions in this section).

**Confidential data**: Any information that requires (by contract, law, ethical guidelines, or data owner mandate) controlled access to a select group of individuals or, any information that could cause harm to individuals or Emory if used inappropriately or disclosed, but is not considered restricted data. In the case of

non-directory student records (as defined by Emory FERPA guidelines), aggregated data containing records for fewer than 500 individuals are considered confidential data. Examples: employee records that do not contain restricted data, Emory-owned proprietary information, a class roster, a spreadsheet of names and addresses of financial donors to Emory, an internal audit report.

**Restricted data**: Any information that, if used inappropriately or disclosed, could cause significant harm to individuals or Emory. This includes information that could be used for identity theft, or information that carries significant penalties if disclosed. Below is a list of items included in this definition. For all items, if the content only references the corresponding computer user then the content can be considered confidential data (e.g. Brad's computer has a file containing Brad's name, address, and social security number).

- Electronic patient health information (ePHI) that has not been de-identified.
- Combinations of Personally Identifiable Information that could readily be used for identity theft:
  - Social security numbers, when combined with any form of the corresponding name
  - Driver's license numbers, when combined with any form of the corresponding name
- Credit/Debit card numbers
- Financial records that could lead to identity theft or fraud (e.g. bank account numbers)
- Non-directory student records for 500 or more individuals
- Human subject research data containing personally identifiable information
- Any data deemed to be restricted by the data owner
- Any data that, if acquired by unauthorized individuals would require notification of affected parties
- Any data that Emory is legally, contractually, or ethically obligated to encrypt
- Passwords to computer accounts with access to internal, confidential, or restricted information.

**Related Links**
Current Version of This Policy: http://policies.emory.edu/5.13

Emory webpage on FERPA, including the definition of "directory information" at Emory - http://www.registrar.emory.edu/ferpa/ferpa.htm

**Contact Information**

| **Subject Conta** | **ct** | **Phone** | **Email** |
|---|---|---|---|
| Clarification of Policy | Chief Information Security Officer | (404) 727-2630 | brad.sanford@emory.edu |

**Revision History**