

**Virginia Commonwealth University  
Technology Services**

**Security Standard for  
Encryption**

**Effective Date:** February 2008

**Compliance Date:** August 2008

**Revision Date:**

Revisions:

Version	Date	Revision Issuance
1	February 2008	Initial version

**Scope:**

This standard is applicable to all confidential data that is used at the University.

**Applied Industry Best Practices of:**

- SANS Software Security Institute
- Center for Internet Security Consensus Security Benchmarks
- National Institute of Standards Technology (NIST)

**Requirements of the Standard**

**S1.0 – All confidential data (see definition below) must be stored on network storage.**

S1.1 – All confidential data must be stored on University network storage. The storage of confidential data on local storage media is prohibited except when following the requirements described in S2.0 below.

**S2.0 – Confidential data cannot be stored locally unless it is authorized and encrypted.**

S2.1 Confidential data that is stored on non-network storage devices (i.e., on desktop computers, laptops and mobile storage devices) must be authorized by the Chief Information Officer (see Request to Store Confidential Data on Local Storage Media at the end of this Standard) and

must be encrypted with a University-approved encryption technology that is described in the Implementation Guidelines.

## Implementation Guidelines

- **Enterprise Encryption**
  - VCU will be implementing an enterprise encryption solution that includes full disk encryption for desktops, laptops and mobile devices. The solution includes a secure centralized management system for administration and distribution of encryption software and keys.
- **Interim Solutions**
  - Recommended free (Open Source) encryption solutions to use before the University-wide enterprise encryption is implemented are as follows:
    - Hard disk encryption – Truecrypt (available at <http://www.truecrypt.org/> )
    - Single File encryption – Omziff (available at <http://www.xtort.net/xtort-software/omziff/> )

## Definitions

Confidential Data - data and resources that must be protected as mandated by federal, state or University regulations. See the [Data Classification Guidelines](#).

## Enforcement

Violation of this standard could result in the disciplinary actions and/or removal of access privileges.

## Exceptions

Requests for exceptions to the requirements of this standard should be made to the VCU Chief Information Officer. Please use the Security Standard Request for Exception form that is located on the VCU security website and send the completed form (by hard copy or email) to the VCU Chief Information Officer.

**Review Frequency:** Annually or as needed

**Authority:** VCU Chief Information Officer  
VCU Information Security Officer

***In Compliance with:***

VCU Academic Policy: Security of Electronic  
Confidential Information  
VCU Academic Policy: Information Security Policy  
COV ITRM Information Technology Security Standard  
SEC501-01  
VCU Computer and Network Resources Use Policy

**Virginia Commonwealth University  
Technology Services**

**Request for Authorization  
To Store Confidential Data  
on Local Storage Media**

This form is to be used to request authorization to store confidential data on local storage media (e.g., hard drives of desktop computer or laptop and mobile device such as a USB drive or CD). In addition to receiving authorization via this form, the data must be encrypted using a University-approved encryption technology.

Please complete all the information below, and send the completed form to the Chief Information Officer with a copy to your department head. The request will be reviewed, and you will be notified of approval.

**Date of request:** \_\_\_\_\_

**Identify Confidential Data Involved:**

---

---

---

**Reason for Need to Store Data Locally:**

---

---

**Description of Local Storage Media and Encryption Being Used:**

---

---

---

**Contact Information:**

<b>Name</b>	
<b>Department</b>	
<b>Email Address</b>	
<b>Phone</b>	

**Explain any extenuating circumstances:**

---

---

---

- Approved**
- Rejected**

**Date:** \_\_\_\_\_

**Authorized Signature of CIO:** \_\_\_\_\_