

Old Dominion University Computer Science Department Policies and Procedures

Title: Data Encryption

ID: CSD002

Revision: 1.0

Purpose

The purpose of this document is to define the required methods used by Computer Science account holders in order to properly encrypt and protect their data.

Scope

This procedure pertains to all members of the Computer Science Department.

Policy

- Sensitive Data

As stated in Policy CSD001 (Sensitive Data Storage), any confidential data is not allowed to be stored on personal devices. When data is stored on a Departmental device, proper encryption techniques are required.

- Non-confidential data

In any other cases, the Computer Science Department does not require the encryption of data, but strongly suggests that each individual does employ such techniques to assure the safe and secure storage of their intellectual property.

- Applicable Areas

The encryption requirements and techniques stated below are applicable to a wide area of devices. This includes mobile devices (USB flash drives, laptops, PDAs, cell phones, etc.), desktop computers, CD and DVD media, external and portable hard drives, e-mails and e-mail attachments.

- Encryption Requirements

The Computer Science Department follows the Office of Computing and Communications Services in their requirements for encryption algorithms and strength of public and private encryption keys. According to the OCCS Encryption Usage and Key Escrow Standard Rev. 6.3.2

Public and private keys must meet the following standards:

- Minimum encryption strength of 56 bit for general use
- Minimum encryption strength of 128 bit for any system that transmits a username and password, unless a written agreement with an entity in a foreign country for a lower standard is in place

- Encryption Software

The Computer Science Department proposes, but does not limit to, a list of encryption software tools. For basic file and folder protection on various Operating Systems the following software tools can be utilized:

7-zip – File and folder encryption.

BitLocker – Boot disk and full disk protection.

Cryptainer LE – Files, folders, and external drive protection.

Disk Images - File and folder encryption.

File Vault- File and folder encryption.

TrueCrypt - Files, folders, and external drive protection.

The Department, would like to point out the fact that proper encryption techniques should be utilized during data transfers to and from network file systems and external devices. Secure protocols must be utilized to transfer data between devices.

Recommended protocols are SCP and SFTP. Recommended tools to be utilized are scp,sftp on *nix and WinSCP on Windows Operating Systems. Servers to be utilized for these protocols are scp.cs.odu.edu and sftp.cs.odu.edu.

Definitions

Encryption: Encrypting or scrambling data to assure confidentiality and integrity.

SCP: Secure Copy. An encrypted protocol for data copying based on the Secure Shell Protocol.

Revision History

1/7/2011 – Rev 1.0 Pending approval by Ajay Gupta