Removable Media Security Policy

Summary

Common uses for removable media devices include transferring files between computers and backing up important files. Removable media devices do not have the same security controls in place as CSU computer systems. Therefore, following the guidelines in this policy is essential.

For the purpose of this policy, removable media devices include, but are not limited to, floppy disks, CD-ROMs, DVDs, jump drives, etc.

Purpose

This policy establishes safeguards for using removable media in conjunction with CSU data and the CSU network. Appropriate security of all removable media, whether owned by Columbus State University or by individuals, is required to prevent the spread of viruses, the loss or compromise of sensitive data, and other risks to the CSU network.

Policy

Removable media may not hold sensitive information; nor should it replace network storage. All CSU information should be stored and accessed from a campus file server where it is physically secure and is routinely backed up to tape.

Users must follow physical security best practices to prevent the theft or loss of removable media and user data. Users often leave removable media in lab computers or, because of their small size, simply misplace them.

Procedures and Responsibilities

Users are responsible for the use of removable media.

UITS does not promote the use of removable media nor take any responsibility for the loss of data on removable media.

Related USG Policy

13.2 (BOR) 13.2 Third Party Software Policy & 5.8 (IT Handbook) Endpoint Security

Last Update

3/18/2014

Responsible Authority

Chief Information Security Officer