Portable Device Security Policy

Summary

Portable computing devices (PCDs) are becoming increasingly powerful and affordable and their small size and functionality makes them popular among computer users. While these devices are extremely convenient, they can also pose a risk to the University network and the confidentiality, integrity, and availability of the data stored therein. Uploading documents that contain viruses and downloading sensitive data are among those risks. There is also the risk of mechanical or electronic failure, damage from being dropped or exposed to weather, or simply being lost or stolen.

For the purpose of this policy, portable computing devices include, but are not limited to, notebook and laptop computers and Portable Digital Assistants (PDAs) such as Palm Pilots, smart phones and the like.

Purpose

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

Policy

- PCDs must use a logon and/or power-on password when technically available. Any device that accesses University systems or information must provide for network authentication. If the PCD is not capable of using the University network authentication method, then a local password is required.
- PCDs may not store sensitive information; nor should they 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 AN storage device and\or tape.
- Users must follow physical security best practices to prevent theft of PCDs and data. Never leave an unattended PCD in the open, especially in a vehicle.
- PCDs must use an up to date antivirus program, when technically available.
- PCD users must follow desktop security standards to the extent technically possible.

Procedures and Responsibilities

- UITS will securely configure all University owned PCDs prior to distribution. Users should arrange with UITS for periodic maintenance and updates.

- Users are responsible for securely configuring personally owned PCDs. UITS reserves the right to refuse a network connection from an insecure device.
- Report PCD theft to the Campus Police and the UITS Help Desk.

Related USG Policy

5.8 (IT Handbook) Endpoint Security & 5.11 (IT Handbook) Minimum Security Standards for USG Networked Devices & 8 (IT Handbook) Bring Your Own Device (BYOD) Standard

Last Update

4/17/2014

Responsible Authority

Chief Information Security Officer