

Waycross College

IT Vulnerability Scanning Policy

Effective Date: March 31, 2007
Last Revised: December 19, 2006

Status:

- Draft
- Approved

Responsible University Officer

Director of Computer Services

Responsible Coordinating Office

Computer Services

Online Publication

<http://www.waycross.edu/compserv/itpolicy/>

1. Scope

This College-wide policy governs the scanning of all devices connected to the campus networks for vulnerability detection. Connecting a device to the Waycross College network (including the student wireless network) may subject your device to vulnerability scanning. It is the user's choice whether to connect to the Waycross College student wireless network. Connecting to the network indicates approval on the part of the user for Waycross College to scan the connected device.

2. Policy

2.1. Vulnerability Scanning

2.1.1. Campus-wide Scanning

- In a campus-wide effort to reduce IT security risks and supplement existing security practices, Computer Services will perform periodic vulnerability assessments on devices connected to the Waycross College network. Computer Services may also scan for vulnerabilities that are being exploited in current attacks.
- Such vulnerability assessments will consist of network scans for open communications ports, detection of host operating systems, and detection of remote applications to identify well-known vulnerabilities or high-risk system weaknesses.

- The assessments will not search the contents of personal electronic files on the scanned computers.
- Scans should not cause interruption to the campus network, though device log files may reflect the scans that take place.