Network Connectivity Policy

Summary

The CSU data communications network consists of:

- Network devices such as switches, routers.
- Wireless access points the wiring between and within each campus building.
- Network services such as DNS and DHCP.

The network provides CSU students, faculty, and staff with the ability to access information resources, collaborate, and communicate. Of utmost importance is the safeguarding of these important information assets and assuring the confidentiality, integrity, and availability of all network resources.

Purpose

The purpose of this policy is to safeguard network resources and prevent network problems by establishing procedures and responsibilities for CSU network administration.

Policy

All users must adhere to the CSU Appropriate Information Systems Use Policy

No one, other than UITS personnel, may connect a network device such as a router, switch, hub, access point or modem to the network.

UITS requires a minimum of 4 working days' notice for installation of additional data lines.

No one, other than UITS personnel, may run a server of any type on the network. No one may tamper with any network component or attempt to circumvent network security.

CSU is not responsible or liable for loss of data due to the use of unsecured protocols such as FTP, Telnet etc. The CSU network prohibits Telnet, FTP, and other unsecured protocols.

All computers connected to the network must authenticate\register with UITS to and obtain a CSU IP address. Under NO circumstances may a computer connected to the network use an IP address other than the one that UITS assigns.

Procedures and Responsibilities

UITS personnel are responsible for all aspects of the CSU network and only those authorized to do so may engage in network maintenance activities.

UITS is responsible for developing network standards and procedures and for configuring, optimizing, troubleshooting, and documenting all network equipment. UITS is responsible for managing the CSU network name space and the assignment of IP addresses for security and identity of users.

Users requiring additional data lines should submit an eQuest request at least 4 working days in advance.

Users should report network problems to the UITS Help Desk.

Related USG Policy

3.3 (IT Handbook) Continuity of Operations Planning & 3.4 (IT Handbook) Network Services & 5.1 Information Security & 5.11 Minimum Security Standards for USG Networked Devices

Last Update

2/4/2014

Responsible Authority

Chief Information Security Officer