

California State University, Fresno

Network Connection Policy

1. Policy

California State University, Fresno requires devices connecting to the network to register, meet security baselines, and be configured not to conflict with centrally provided services. Devices connecting to the network must meet the conditions outlined in this policy.

2. Reason

The purpose of this policy is to safeguard and ensure the reliability and availability of the California State University, Fresno network by defining the requirements for connectivity of devices. Network availability, integrity, and security are at risk when non-compliant devices connect to the network. Devices in compliance with this policy are less likely to disrupt the network or interfere with other connected devices.

3. Scope

All staff, faculty, and students of California State University, Fresno, guests, third parties, and any other entities connecting any device to the network are subject to this policy.

4. Registration

Devices connecting to the network require registration. Registration, at minimum, identifies an appropriate contact for the device connecting to the network. Periodic registration renewal is necessary to maintain up-to-date information of devices connected to the network.

5. Security

Devices connected to the network must meet the minimum baseline security¹ device requirements established by the University. Implementation of these security requirements for devices protects the device and reduces the security risks to other devices on the network.

6. Services

Devices connected to the network must not run services that disrupt or interfere with network enabling services provided centrally. Network enabling services are layered services supporting the connecting of a device to the network.

7. Extensions

Any device connected to the network that provides connectivity to other devices requires approval. Such approved extensions from the President's designee are available only to colleges or departments of California State University, Fresno and require adherence to the University's policies and standards and Executive Orders from the Chancellor Office's.

8. Compliance

Users connecting devices to the network consent to compliance verification of this policy. The compliance verification process for devices is limited to configuration and security inspection and follows University policies protecting privacy.

9. Disconnection

Devices are subject to disconnection from the network for infractions of this policy which pose a threat to other devices.

¹ See Minimum Security Baseline Policy For Network Connected Devices

APPROVED:



JOHN D. WELTY

DATE 9/20/06

Recommended by IETCC 8/31/06