Practice On Enforcement Of Unauthorized Campus Network Extensions

Audience
All members of the Fresno State community or visitors who have any device connected to the Fresno State network.

Definition
Extensions of the campus network infrastructure include the use of wired equipment, wireless devices or wireless access points, leased lines or dedicated facilities, which extend the campus network, allow remote access to University systems or services, or access to off-campus locations or other networks.

Policy Statement
The Network Connection Policy[1] prohibits, without appropriate approval, extensions of the university network. Any type of device designed to extend network access is not permitted without appropriate authorization.

Background
The issues surrounding extending the campus network infrastructure include security and accountability. All means of extending the campus network are potentially incompatible with these issues.

Fresno State must be able to keep secure its data and technology resources. Unauthorized extension of the campus network to remote facilities or interconnecting to other networks is a serious security threat.

Security concerns involve protecting university data, computers, and the network from unauthorized use. A primary security risk posed by devices that extend the campus network is exposure and possible interception of sensitive data.

Fresno State must be able to document and account for network resource access and utilization to meet increasing regulations. These regulations and standards include:

- Protection of credit card holder information, such as the Payment Card Industry (PCI) Data Security Standard
- Protection of personal privacy, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Educational Rights and Privacy Act (FERPA)
- Protection of intellectual property rights, such as the Digital Millennium Copyright Act (DMCA)

Unauthorized extension the network infrastructure limits the University's ability to secure the data flow end-to-end and to understand the security requirements.

[1] https://www.fresnostate.edu/adminserv/technology/documents/network_connections_policy.pdf

Process

The following procedures facilitate the detection, analysis, mitigation, and disconnection of unauthorized devices that extend the non-residential campus network.

Detection

- On a regular basis, or quarterly, Technology Services (Network Engineering) will conduct scans of the campus network and gather relevant log records to write the resultant information into a database. The database will include fields to indicate:
    a. Unknown wireless access points and their configured SSID
    b. Unknown/new devices that extend the network

Analysis

- On a regular basis, or quarterly, Technology Services (Information Security) will review the information in the database for changes and initiate mitigation procedures for unknown devices.

Mitigation

- Technology Services (Information Security) will create a ticket in the problem tracking system and send device details and a policy notice (via e-mail) regarding the unauthorized device to:
    a. Executive Director of Technology Services
    b. Appropriate manager of area where the device is installed
    c. The owner or operator of the device, if known
- Technology Services (Information Security) will allow one week for a response detailing which remediation or mitigation steps have been taken:
    a. The device was removed
    b. Appropriate approval for connection of the device
- Technology Services upon unsatisfactory responses or any subsequent detection of the device, in any location, after one week from sending the notice will disconnect the device extending the network.

Disconnection

- Technology Services, in accordance with the Disconnect Policy[2], may disconnect devices, including devices that extend the network, in an emergency to prevent catastrophic damage and protect university data and technology resources. Technology Services, as soon as practical, would inform and consult with units affected by such an emergency.

Enforcement

It is important that unauthorized extensions to the campus network infrastructure be removed in accordance with previously established University policies. The removal of unauthorized network extensions will allow the University to maintain a secure and reliable network.

---

[2] https://www.fresnostate.edu/adminserv/technology/policies/disconnect.html