

California State University, Fresno
Minimum Security Baseline Policy For Network Connected Devices

1. Policy

California State University, Fresno requires devices connecting to the network to meet the minimum security baseline in order to protect devices. Devices connecting to the network must comply with the minimum security baseline before access to university information resources is granted.

2. Reason

The minimum security baseline safeguards protect the confidentiality, integrity, and availability of each individual device and other devices connected to the network by reducing the security susceptibility of every device.

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. Minimum Security Baseline

All network connected devices able to must be configured to meet the minimum security baseline. The baseline security safeguards listed below are the minimum required to protect devices.

Anti-virus software must be enabled, running, and up-to-date on every device.

The built-in (native) firewall of a device or a more advanced firewall must be active. Firewall configurations must permit and allow for policy compliance verification.

Applications and operating system software running on devices must be a supported version.

The installation of relevant software updates, patches, or upgrades fixing critical or high security vulnerabilities of devices must be prompt.

5. Compliance

Users connecting devices to the network permit and consent to verification of compliance with this policy.

6. Exceptions

Users connecting devices to the network, which are unable to meet the requirements of this policy, must obtain an exception from the chair of STLT.

7. Enforcement

Devices are subject to disconnection from the network for infractions of this policy which put other devices at risk.

Recommended by IETCC 8/31/06