The Pomona College system employs cryptographic controls in accordance with applicable Federal 6TþO/CS0 cs 0 0 0 scn/TT2 4e( )8( )-204.2( )-10.812c68.2( )]TJ(c)

The Pomona College system terminates the network connection associated with a communication session at the end of the session or after 10 minutes of inactivity

Pomona College:

Establishes usage restriction and implementation guidance for Voi

Monitoring all traffic leaving Pomona College and detect for any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices.
Requiring that confidential information be stored only on Pomona College-controlled system components, storage devices, personally owned devices configured in accordance with the Pomona College Mobile Device policy[3], or third-party storage services

DATA INTEGRITY

Pomona College utilizes integrity checking mechanisms to detect unauthorized changes to Pomona College hardware software, firmware, and information. Unauthorized changes to hardware software, firmware, and information can occur due to errors or malicious activity.
Pomona College systems perform integrity checks of hardware software, firmware, and information
- Periodically
- Upon occurrence of a security related event such as:
  - Identification of a new threat to which Pomona College is susceptible
  - Installation of new hardware
  - Installation of new software
  - Installation of new firmware
- Upon entering a transitional state, such as:
  - System startup
  - Restart
  - Shutdown

Pomona College incorporates the detection of unauthorized changes to the system into the incident response process

DEVELOPMENT ENVIRONMENT

Where applicable, Pomona College maintains a baseline configuration for system development and test environments that is managed separately from the Pomona College production baseline configuration.

Establishing separate baseline configurations for development, testing, and production environments helps Pomona College protect its system from unplanned and unexpected events related to development and testing activities.
Separate baseline configurations allow Pomona College to apply configuration management that is most appropriate for reach type of configuration.

[3] See Pomona College Mobile Device policy