ix. Turn on audit capabilities on AP; review log files on a regular basis.
x. Only wireless APs expressly authorized by the Security Officer shall be permitted to establish a connection.

c. Mobile Systems
   i. Install anti-virus software on all wireless clients.
   ii. Install personal firewall software on all wireless clients.
   iii. Disable file sharing between wireless clients.
   iv. All wireless devices shall be identified and authenticated prior to establishing a connection.

Violations:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Violation may also result in civil and criminal penalties to [Insert Company name] as determined by federal and state laws and regulations related to loss of data.

Attachments: None

Related Policies: Use of Mobile Devices

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.