CHAPTER 21

WIRELESS ACCESS AND USE

MARCH 2015

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 21

WIRELESS ACCESS AND USE

1. PURPOSE. The purpose of this chapter is to provide policy regarding authorized access and use of wireless technologies on or within California Highway Patrol (CHP) premises to secure and protect the information assets owned by the CHP and the State of California. Any questions or comments about this policy should be directed to Information Management Division (IMD).

   a. The CHP provides computer devices, networks, and other electronic information systems to meet its mission, goals, and initiatives. The CHP grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. Misuse of computing, networking, or automated information resources may result in loss of computing privileges and may be cause for disciplinary action and/or prosecution under applicable state or federal statutes.

2. SCOPE. All CHP employees and non-departmental staff (consultants, contractors, temporary/volunteers, and all personnel affiliated with third parties), hereafter called "Users," who access CHP wireless infrastructure must adhere to this policy. This policy applies to all wireless infrastructure and devices that connect to a CHP network or reside on a CHP site that provides wireless connectivity to endpoint devices including, but is not limited to, laptops, desktops, smart phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

NOTE: Any exemption to this policy requires advance approval from IMD and is subject to the recommendation of the Information Security Officer (ISO).

3. POLICY. Use of wireless technology enables the convenience of mobility to CHP's internal network and/or dedicated Internet access (separate from CHP's internal network) where wireless coverage is available.

   a. Wireless Access Point.

      (1) Authorized Wireless Access Point. Information Technology Section (ITS) is solely responsible for installing, configuring, and maintaining wireless access, wireless infrastructure, and wireless networking services on all CHP premises for any purpose. No other Wireless Access Points (WAP) or wireless hotspot devices are permitted to be installed or connected to the CHP network or used for Internet access to CHP information assets/equipment on CHP premises.

(a) The location of all departmental WAPs on CHP premises statewide shall be recorded and maintained by ITS.

(b) All WAPs shall require User authentication at the access point before granting access to the CHP internal network or dedicated Internet services.

(c) Outside vendors, agencies, or other departmental guests, hereafter called "Guests," requiring Internet access for presentation or business purposes may use the dedicated, or Guest, wireless Internet service where available. In locations where Guest wireless Internet service is not available, Guests may temporarily use Guest supplied WAPs or a wireless hotspot device to establish Internet connectivity to their equipment; not to CHP information assets/equipment.

(2) Unauthorized Wireless Access Point. No Users shall create unauthorized wireless networks to access the CHP internal network or Internet services on CHP premises. No User on CHP premises shall connect CHP equipment to non-departmental wireless networks or Internet services.

(a) This includes establishing WAPs, wireless routers, or open networks on personal devices (with the exception of temporary Guest WAPs/hotspot devices).

(b) All other WAPs emanating from Department property must be installed, configured, and maintained by ITS and have ISO approval prior to activation.

(c) Identified unauthorized WAPs emanating from Department property determined to be hostile (compromising or significantly interfering with the internal CHP network and/or resources) will be disabled immediately.

1 The owner of an unauthorized WAP is considered to be in violation of this policy and may be subject to disciplinary action.

b. Wireless Access.

(1) California Highway Patrol Internal Wireless Network Access. Wireless networking is deployed by ITS and provides Users access to the CHP internal network automatically from properly configured departmental wireless enabled equipment.

(2) Guest Wireless Internet Access. Also deployed by ITS, Guest wireless Internet access (separate from the CHP's internal network) is available as a convenience for Users and Guest access.

NOTE: This service is not available on all CHP premises. Contact your Division Network Administrator (DAdmin) or the CHP Help Desk at (916) 843-3899 to determine availability and/or receive access instructions.

c. Acceptable Use. The CHP wireless network infrastructure is a shared and limited resource. All users have an obligation to use this resource responsibly. Only Users affiliated with the CHP are authorized to use wireless networking on CHP premises.

(1) Use of California Highway Patrol Internal Wireless Network. Internal CHP wireless network access is provided for business purposes only.

(a) Wired, or wireless, connectivity of non-departmental equipment to the internal CHP network is strictly prohibited.

(b) Any exemption to this policy requires advance approval from IMD and is subject to the recommendation of the ISO.

(2) Use of Dedicated "Guest" Wireless Internet Access. Intermittent employee, non-departmental, and guest use of the dedicated "Guest" wireless Internet is acceptable when consistent with the Department's Acceptable Use Policy (refer to Chapter 18, Acceptable Use Policy, paragraph 3.a., of this manual).

(a) The Department assumes no responsibility for the loss, theft, and/or damage (physical or intellectual) to any personal device that a User connects to the CHP network.

d. Support.

(1) Information Technology Section will regulate and manage all WAPs and radio frequency bands used by wireless technology to ensure fair and efficient allocation, and to minimize collision, interference, unauthorized intrusion, and failure of the wireless network.

(2) Wireless networks should be designed and deployed to avoid physical and logical interference between components of different network segments and other equipment. In the event a wireless device interferes with other equipment, ITS will resolve the interference as determined by use priority.

(3) Users are responsible for configuration and maintenance of personal device(s) which they connect to the dedicated wireless Internet. The Department will not provide information technology support for User's personal devices.

e. Security.

(1) Information Technology Section will attempt to resolve any interference or security incidents by coordinating with the appropriate DAdmin. If a DAdmin is not available, the incident may be resolved through network administration from headquarters.

(2) Information Technology Section is authorized to take whatever reasonable steps are necessary to ensure compliance with this policy and other network related policies that are designed to protect the integrity and security of the CHP's network.

f. Disconnect Authorization. Any wireless access to the CHP network and/or network resources which poses a security threat (i.e., hostile) may be disconnected.

(1) If a serious security breach is in progress, if necessary, ITS may immediately disable wired connectivity to the network. Every reasonable attempt will be made to reach the DAdmin to assist in resolving security issues and departmental notifications shall be made.

(2) Information Technology Section has the authority to disconnect any wireless devices connected to the CHP's network infrastructure which has been identified as unauthorized, hostile, and/or whose traffic violates practices set forth in this policy or any other network related policy.

(a) A hostile disconnect requires post notifications to IMD, ITS, ISO, DAdmin, and the local command.

(b) A non-hostile disconnect requires advanced authorization from IMD, ITS, and the ISO. Advanced disconnect notification will be provided to the DAdmin and local command.

g. Privacy. The Department monitors network activity. This includes, but is not limited to, sites visited, content viewed, and electronic mail sent and received.

(1) Users should have no expectations of privacy when using these resources.

(2) Internet usage records may be used in investigative processes.

4. ENFORCEMENT. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Violation of this

policy by non-departmental staff (contractor, consultant, vendor, or temporary/volunteer worker) may result in the termination of their services or assignment with the CHP.

5. DEFINITIONS.

a. California Highway Patrol Internal Wireless Network. Local area network (LAN) technology that uses radio frequency spectrum to connect computing devices to departmental wired networks and may connect to the CHP's network backbone and/or the Internet.

b. California Highway Patrol Dedicated Wireless "Guest" Internet. Local area network technology that uses radio frequency spectrum to connect computing devices to Internet services outside of the CHP internal network.

c. Wireless Access Point. Electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub that is used to connect segments of a LAN, using transmit and receive antennas instead of ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and can be connected to the wired network, allowing access to the campus network backbone.

d. Wireless Infrastructure. Wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

e. Coverage. The geographical area where a baseline level of wireless connection service quality is attainable.

f. Interference. The degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.

g. Privacy. The confidentiality of communications and departmental data transmitted over a wireless network.

h. Information Asset or Equipment. Information that is collected or produced, as well as underlying hardware, software, services, systems, and technology necessary for obtaining, storing, using, and securing information recognized as important and valuable to the Department.

THIS PAGE INTENTIONALLY LEFT BLANK