CHAPTER 20

SECURITY AUDITING

MAY 2015

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 20

SECURITY AUDITING

1. PURPOSE. The purpose of this policy is to advise users of security scanning/auditing procedures and precautions used by the California Highway Patrol (CHP) to audit departmental systems and networks to help identify if departmental information or resources have been compromised, have been attempted to be compromised, are currently being compromised, or are vulnerable to compromise. Other persons or entities, unless authorized, are prohibited from performing any such audits.

a. Audits may be conducted to:

(1) Ensure the integrity, confidentiality, and availability of information and resources.

(2) Investigate possible security incidents to ensure conformance with departmental policies, outside agency (state, federal, etc.) policies, or as part of an investigation.

(3) Monitor user or system activity where appropriate.

2. SCOPE. This policy covers all computer and communication devices owned or operated by the CHP, any computer or communication device utilizing CHP network resources, any computer or communication device which has been connected to the CHP network if it is believed such computer or communication device has been used contrary to any CHP information technology policy while connected, and all computers and communication devices that are attempting in any manner to interact or interface with the CHP network or communications system. There is no right or expectation of privacy on CHP networks, systems, devices, and/or media; unauthorized access or use is strictly prohibited and may be punishable under Section 502 of the California Penal Code.

3. POLICY. California Highway Patrol staff having appropriate network security administrative responsibilities shall utilize auditing software to perform electronic scans of networks, servers, switches/routers, firewalls, and/or any other systems at the CHP. This also includes scans/audits of any electronic communication and electronic mail (e-mail) regardless of sender or recipient of communication(s). Any suspicious activity shall be reported to the Information Security Officer by telephone at (916) 843-4000 or e-mail at ISO@chp.ca.gov.

a. Electronic scans/audits may include, but are not limited to:

(1) User and/or system level access to any data, network system, or communications device; this includes network systems, network infrastructure, personal computers, laptops, portable devices, e-mails, instant messaging, etc.

(2) User, system, and/or administrator events; this includes account logons, account management, directory service access, object access, group policy change, use of privilege/administrative access, any network change processes, etc.

(3) Access to work areas; this includes labs, offices, cubicles, storage areas, etc.

(4) Access to interactively monitor and log traffic on CHP information and communications networks.

(5) Penetration and vulnerability testing.

(6) Account and password auditing.

(7) Scanning for personally identifiable information.

4. NETWORK CONTROL. Internal security scanning on all CHP-owned networks requires the prior approval of the Chief Information Officer. This includes all devices and infrastructure connected to the network at the time of the scan.

5. DEFINITIONS. Connection(s) to the CHP network may include, but is not limited to, the following:

a. Network Infrastructure Connection. Having a wired network capable device; this includes a laptop, desktop, portable device, etc., plugged into a functioning network port within a CHP owned/operated facility.

b. Wireless Network Infrastructure Connection.

(1) Having a CHP wireless device; this includes a laptop/mobile digital computer, mobile phone, portable device, etc., connected to a CHP Wireless Access Point (WAP).

(2) Having a personal wireless device; this includes a mobile phone, laptop, tablet, etc., connected to a CHP WAP.