CHAPTER 2

NETWORK SECURITY AND ADMINISTRATION

REVISED DECEMBER 2024

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2

NETWORK SECURITY AND ADMINISTRATION

1. GENERAL.

a. The CHP network is to be used for business purposes only. Employees and other computer users shall use network resources only in the course of conducting approved business activities.

b. The provisions of this chapter apply to all departmental networks, systems, applications, and related data.

2. SECURITY AGREEMENT.

a. The CHP 101, Appropriate Use of Automated Information & Systems Statement, has been developed to improve security procedures and can be found on the CHP Intranet site under Forms.

b. Commanders shall ensure a CHP 101 is completed by all individuals who have access to the Department's network resources.

c. Current Employees.

(1) State employees and others who access or are likely to access a CHP computer system, network, or information generated by these resources shall read and sign a CHP 101 on an annual basis. This includes Department employees, employees of allied or other state agencies, consultants, student assistants, and volunteers. Employees will sign the CHP 101 in the presence of their immediate supervisor during the annual performance review process.

(2) The CHP 101 process is not required for the general public or other persons who have "read only" access to departmental information through the CHP's Internet website.

d. Potential Employees.

(1) Commands shall inform potential hires that signing a CHP 101 is a condition of employment before hiring commitment is made.

(2) The new hire shall read and sign the CHP 101 in order to complete the appointment process.

e. Copies of signed CHP 101 documents shall be retained in the employee's field personnel folder or other location specified by the commander for three years rotating. Commands shall retain the current signed CHP 101, and the two previously signed copies, to document prior admonishments.

f. Similar policies have been incorporated into other departmental documentation to assist commanders in the performance of security responsibilities.

(1) Language in Highway Patrol Manual (HPM) 10.3, Personnel Transactions Manual, Chapter 2, Nonuniformed Hiring and Appointments, requires hiring supervisors to ensure the applicant is aware that signing a CHP 101 is a condition of employment.

(2) Language on the CHP 128, Request for Personnel Action, indicates a CHP 101 is required to complete the appointment process.

(3) Language on the CHP 137C, Field Personnel Folder Annual Review (Uniformed), identifies the CHP 101 as a form that shall be read and signed by employees annually.

(4) Language in HPM 10.3, Chapter 30, Personnel and Medical Files, instructs commands to file the CHP 101 in the employee's field personnel folder.

g. Nonemployees, Volunteers, or Temporary Employees.

(1) Prior to granting access to CHP resources, a CHP 110, Confidentiality Agreement, must be signed by, but not limited to, the following parties:

(a) Vendors.

(b) Contractors.

(c) Volunteers.

(d) Temporary employees.

(e) Allied agencies.

NOTE: The CHP 110 will be kept on file by the Office of Primary Interest (OPI) for a period of three years after the termination of the joint business venture.

3. PRIVACY ON THE NETWORK.

a. Material generated through use of the CHP network is the property of the State of California. Employees and others who use the Department's network resources shall not consider their activity to be private.

b. The Department may monitor and log network activity, including e-mail activity, without the knowledge or consent of an employee or computer user.

c. The Department's network resources may only be used in the course of conducting approved departmental business.

d. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit (e.g., thumb drives, personal digital assistants and other hand-held peripherals, CDs—Read-Only Memory).

4. DEPARTMENTAL LIABILITY. The Department makes no warranty—expressed or implied—for the service that is the subject of policies in this manual. Additionally, the Department is not responsible for any damages whatsoever which employees or other computer users may suffer arising from, or related to, their use of any state agency electronic information resources, whether such damages be deliberate, incidental, consequential, or otherwise, or whether such damages include loss of data resulting from delays, intentional acts, nondeliveries, mistaken deliveries, or service interruptions whether caused by a state agency's negligence, errors, or omissions. Computer users shall recognize the use of state agency electronic information resources is a privilege, and the policies implementing usage are requirements that mandate adherence.

5. ADMINISTRATION.

a. Network Environment. The CHP network is a statewide system of local area network (LAN) environments. The system is administered by Information Management Division (IMD), Technology Infrastructure Section (TIS), Network Security Group, through a multifunctional team of administrators who plan, install, and support the Department's LAN infrastructure. Accordingly, IMD shall serve as the OPI for all servers attached to the departmental network. As such, no new server may be connected to the network or placed into production prior to meeting all security guidelines, and only upon obtaining approval from IMD. This includes all development, test, and desktop servers with network connectivity. Prior to IMD approving any new server connection, the Department Information Security Officer (ISO) will review the scan of the server to ensure all unnecessary vulnerabilities have been removed. Requests for approval should include the following information:

(1) Internet protocol address.

(2) Media access control.

(3) Port assignment (ports and services required).

(4) Statement that all unneeded ports and services are closed and/or removed.

(5) Administrator and back-up.

(6) Physical location of server.

(7) Physical security implemented.

(8) Emergency contact information (both technical and user management).

[redacted]

(10) System supported, including maximum allowable outage.

(11) Shutdown script (if applicable).

(12) Recovery process.

(13) Classification of data stored on the system.

b. Headquarters Administrators. The Network Administrators who report to IMD are referred to as Systems Administrators. These individuals are located in Sacramento.

(1) Systems Administrators have ultimate responsibility for securing the computer systems they administer and maintain. Individuals assigned these responsibilities will ensure the commonly accepted security practices detailed in paragraph 7. of this chapter are followed, and that extra precautions are taken to eliminate vendor-issued (default) and hard-coded passwords. Moreover, passwords yielding access to administrator-equivalent accounts shall not be compromised in any way.

(a) Each server attached to the CHP network shall include documentation of the baseline configuration. This documentation shall be completed by the respective System Administrator and updated whenever there is an authorized change to the server. The System Administrator is responsible for periodically reviewing [redacted] the server configuration to ensure no unauthorized changes have been applied.

(b) Operating system upgrades shall be reviewed by the respective System Administrator for appropriateness and impact. The TIS commander, in conjunction with the Department ISO, will approve all

upgrades prior to installation. Once approved, the respective System Administrator shall thoroughly test all proposed modifications and develop an installation strategy. The TIS commander will verify sufficient testing has been completed and approve the installation strategy.

[redacted]

c. Firewall Administrator. A firewall is a computer acting as a gateway, which insulates an internal network from the Internet and acts as a gatekeeper, overseeing the flow of data in and out of the internal network, as well as between resources within the internal network. The Department's Firewall Administrator, who reports to TIS, programs instructions that govern how this gateway handles network traffic. The Firewall Administrator also serves as the TIS coordinator for network security issues and interacts directly with the Department ISO.

(1) Each firewall attached to the CHP network shall include documentation of the baseline configurations. This documentation shall be completed by the Firewall Administrator and updated whenever there is an authorized change. [redacted]

(2) Firewall upgrades and/or rule-set modifications shall be reviewed by the Firewall Administrator for appropriateness and impact. The TIS commander, in conjunction with the Department ISO, will approve all upgrades/modifications prior to installation. Once approved, the Firewall Administrator shall thoroughly test all proposed modifications and develop an installation strategy. The TIS commander will verify sufficient testing has been completed and approve the installation strategy.

d. Router Administration. A router controls network traffic and determines where the traffic is sent. It also has filtering capabilities for limiting traffic based on specific predefined rule-sets.

(1) Each router attached to the CHP network shall include documentation of the baseline configuration. This documentation shall be completed by the Network Support Unit (NSU) within TIS and updated whenever there is an authorized change. The NSU and the Department ISO are responsible for

periodically reviewing [redacted] each configuration to ensure no unauthorized changes have been applied.

(2) The Firewall Administrator may also participate in the definition of rule-sets to filter traffic at routed interfaces, as necessary, to protect sources not isolated by firewalls. Rule-sets which are implemented by the NSU at the recommendation of the Firewall Administrator should not be modified unless the modifications have been reviewed and approved by the Firewall Administrator.

(3) Router upgrades and/or rule-set modifications shall be reviewed by the NSU for appropriateness and impact. The TIS commander, in conjunction with the Department ISO, will approve all upgrades/modifications prior to installation. Once approved, the NSU shall thoroughly test all proposed modifications and develop an installation strategy. The TIS commander will verify sufficient testing has been completed and approve the installation strategy.

e. Field Administration. Division Network Administrators (DAdmin), Area Network Coordinators, and headquarters Network Coordinators report to and take direction from TIS but work for commands outside of IMD. These persons play a critical role in supporting the Department's infrastructure of networks. They also perform other duties under the direction of the commander of their respective field Division.

f. Patch Management. System Administrators are responsible for applying software patches to the system in which they have administrative responsibilities.

(1) Patches may be received directly from the respective vendor via Internet downloads or computer media.

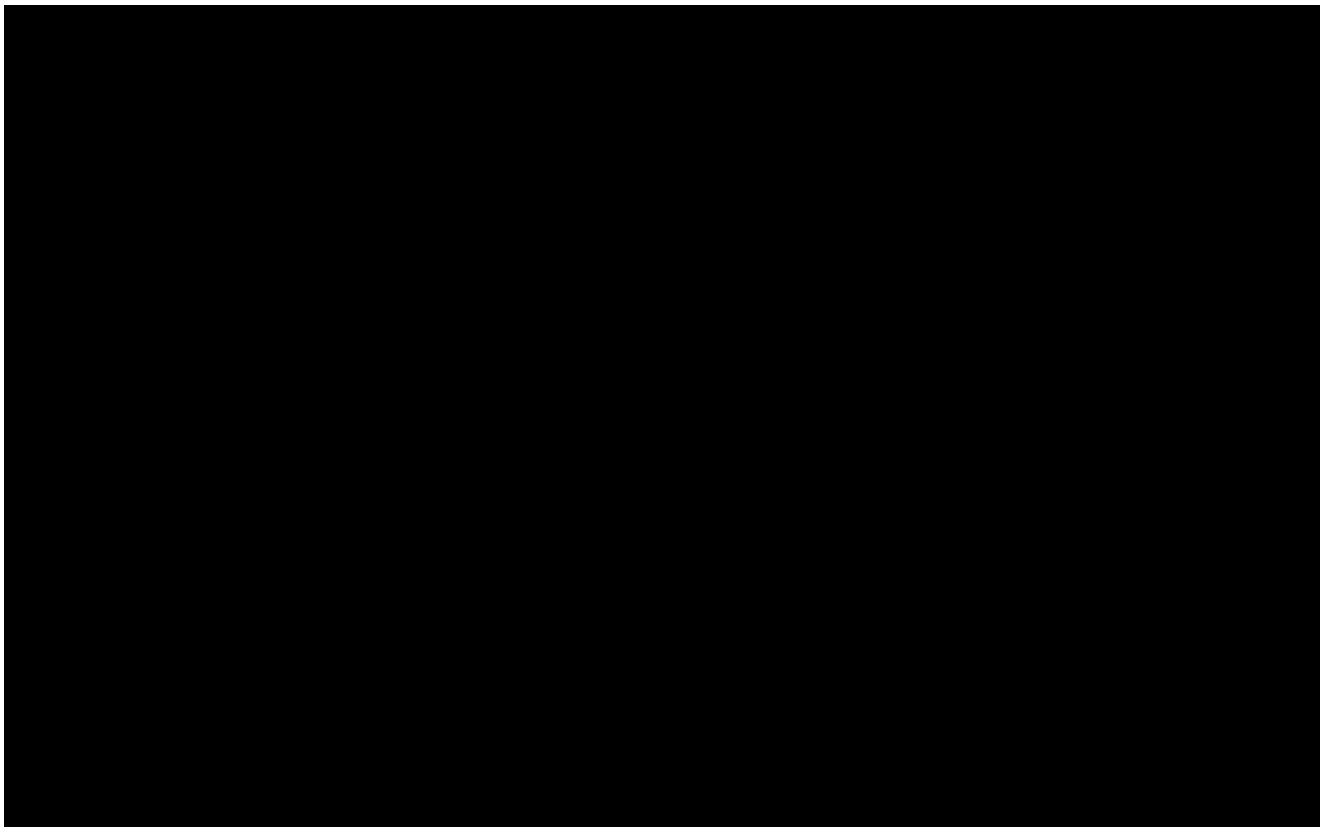
(2) Routine patches will be thoroughly tested and applied on a monthly schedule through normal distribution methods.

(3) High priority patches, as defined by the Department ISO or the TIS commander, will be tested and applied as soon as possible given operational considerations.

(4) The Department ISO will issue ISO Alerts when patch warnings are received from credible sources.

[redacted]

6. NETWORK ACCESS CONTROL.



(5) Non-California Highway Patrol Accounts. Users in this category are not CHP employees and maintain access only to the information repository required to perform an approved specific task. The Department ISO must approve the assignment of these accounts.

b. Employees may gain access to specific CHP computer/information system resources by completing the appropriate Access Request form in ServiceNow (https://chp.service-now.com).

c. Access to Information Belonging to Others. The network stores information on file servers. Each file server stores information on a hard disk. The information stored on the network is organized using a standard directory structure and includes a component called Groups. The CHP defines Groups by the location code of a command, or by the employee's rank, authority, or assignment.

(1) Requests to access a specific document(s) or file(s) from another Group shall be requested via the appropriate Access Request form in ServiceNow. The request will be routed to the Network Administrator who will ensure the requesting employee has their supervisor's and the Group's authorization to access the document/file before permitting the user access.

(2) Requests shall be initiated via the appropriate Access Request form in ServiceNow, be created by the supervisor of the Group into which the

employee is seeking access, and indicate the requesting individual has been granted authority to access the specific document(s) or file(s).

7. PASSWORD MANAGEMENT. Password management is an essential part of effective computer security.

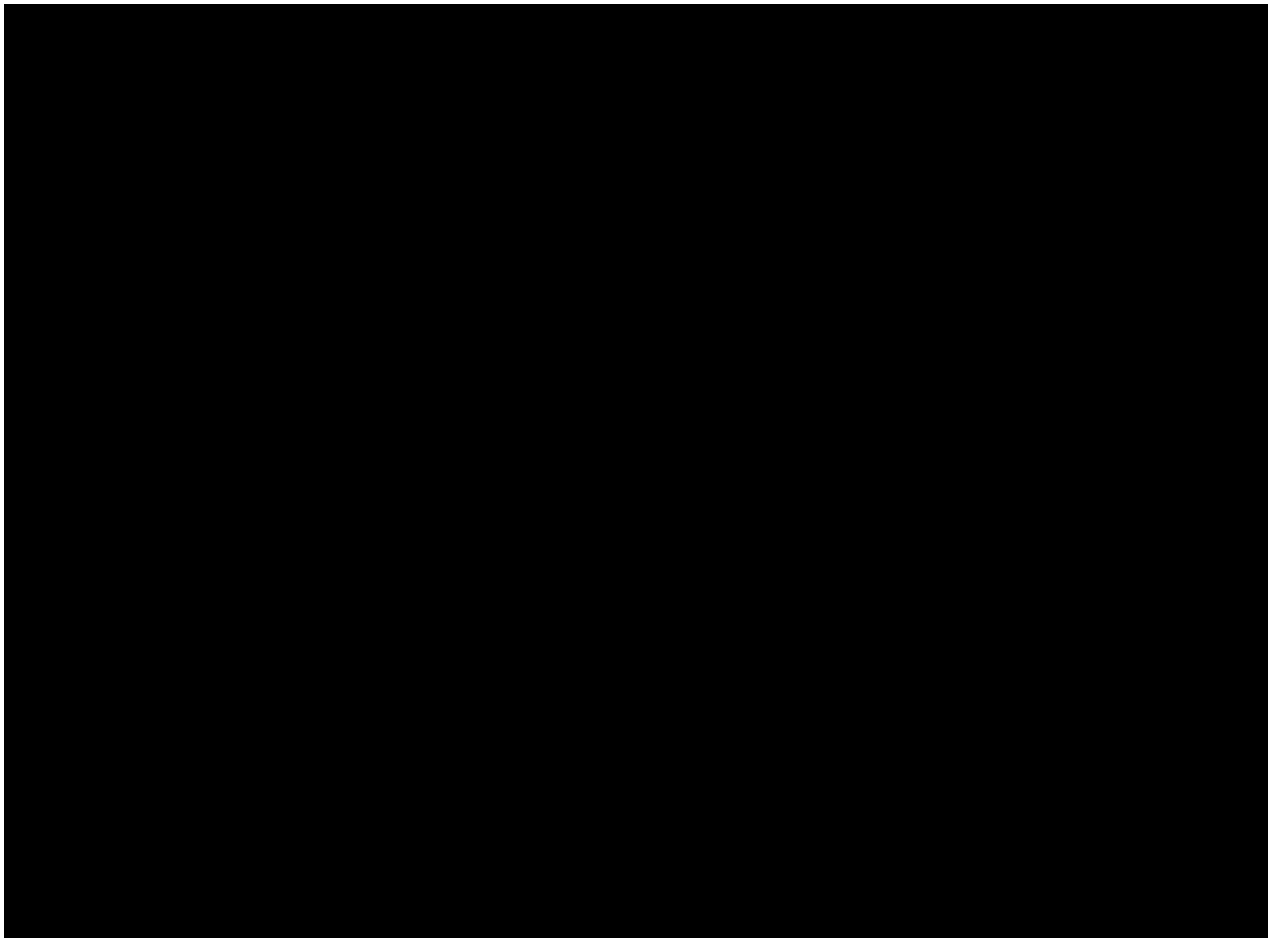
a. Operating System Constraints. For each individual account, the network's operating system enforces the following constraints:

(1) A password is required to access each individual account.

(2) There shall be a single user for each individual access account, and each user shall have their own password. Passwords shall not normally be shared among multiple users.

(3) Passwords shall not be recorded and affixed to computers, monitors, keyboards, etc. Passwords are to be memorized.

(4) Passwords shall have a defined date when they expire.



[redacted]

b. Generic Passwords. Generic passwords (allowing multiple users to access a single account) are not permitted. Exceptions to this policy may be made in situations where the issuance of a generic password is necessary to facilitate an emergency operation only after review and approval by the Department ISO.

c. "Power On" Passwords.

(1) The use of "power on" passwords, commonly referred to as Basic Input/Output System passwords, is not normally permitted on departmental computers.

(2) Request for exception shall be forwarded, through channels, to the Department ISO, who will examine the circumstances of the request and make a determination.

d. Forgotten Passwords. The Information Technology (IT) Support Unit is responsible for resetting passwords for all network users, regardless of command or location. The IT Support Unit can be contacted via ServiceNow, or by telephone at (916) 843-3899.

(1) Users should contact the IT Support Unit directly for assistance using one of the methods above. The IT Support Unit will create a temporary password and provide it to the user. The user should immediately log into the network using the temporary password and create a new password when prompted.

e. Hard Disk Encryption Passwords. The hard drives in the CHP's personal computers and laptops are encrypted to secure access against unauthorized users and to protect the data they contain in the event of loss or theft. A password is utilized to gain access to the computing resource when the device is powered on.

(1) Encryption Software Administrator. A single individual shall be designated as the Encryption Software Administrator.

(2) User Passwords. Devices that are shared between functional groups may have a common password, at the discretion of the Department ISO. Shared passwords shall be solely for the purpose of authenticating the encryption system and shall not grant access to the operating system or any network

assets. The user password shall not grant access to decrypt, make changes to, or uninstall the encryption software. This password shall be known to individuals within the appropriate functional group and to any other individuals defined by the Department ISO.

(3) Local Administrator Passwords. A local administrator password shall be implemented which grants designated administrators access to modify and/or uninstall the encryption software for data recovery purposes.

(a) A different password shall be defined for use within each field Division; one password shall be defined for use within all headquarters Divisions.

(b) Each field Division password shall be known only to the appropriate field DAdmin as defined in paragraph 5.e., of this chapter, and to the Encryption Software Administrator.

(c) The headquarters password shall be known only by the Department ISO-designated headquarters Administrator.

(d) Additional individuals may be granted this password at the discretion of the Department ISO. No other individual may be told any local administrator password.

(4) System Administrator Password. A system administrator password shall be implemented which grants access to modify and/or uninstall the encryption software on any CHP computing resource. This password shall be known only to the Department ISO and the Encryption Software Administrator. Additional individuals may be granted this password at the discretion of the Department ISO.

[redacted]

b. Back-Up Responsibilities. The Technology Services Group is responsible for the following back-up activities:

(1) Protecting all business-critical data.

(2) Monitoring the back-up console to assure back-up processes have been successful.

(3) Correcting any problems quickly and efficiently and addressing any problems associated with a back-up process.

c. Recovery. Data will be restored when any primary data failures occur. Primary data failures can be the result of hardware or software failure, data corruption, or human-caused events, such as accidentally deleting a file or document.

THIS PAGE INTENTIONALLY LEFT BLANK