CHAPTER 3

E-MAIL

REVISED JUNE 2026

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3

E-MAIL

1. GENERAL.

a. E-Mail System Defined. An e-mail system is a digital communication platform that enables the exchange of messages through electronic devices such as computers and smartphones. It allows users to send, receive, store, and manage e-mail, and often includes attachments such as documents, images, and links. E-mail systems typically consist of various components including e-mail clients (software to access e-mail such as Microsoft Outlook) and mail servicers (systems that store and deliver e-mail such as Microsoft Exchange).

b. Unintended Visibility. Information contained in e-mail messages may be visible to unintended recipients. Therefore, all users should take appropriate steps to ensure the integrity and security of all messages.

c. Information Quality Assurance Program. The purpose of the Information Quality Assurance Program (IQAP) is to ensure all departmental e-mail users are complying with departmental policy when using the Department's e-mail system as defined in paragraph 2. of this chapter, and to identify users who are sending and receiving excessive, inappropriate, and/or nonbusiness-related e-mail.

d. California Public Records Act Requests. All requests for e-mail records, under Section 7920.000 of the Government Code, California Public Records Act, shall be in accordance with Highway Patrol Manual (HPM) 11.1, Administrative Procedures Manual, Chapter 13, Information Disclosures – Public Records and Rights of Privacy, and shall be forwarded to the Office of Legal Affairs via e-mail at PublicRecords@chp.ca.gov.

2. POLICY.

a. For Business Use Only. All CHP users may use e-mail to correspond with others in the course of conducting official departmental business. It is the responsibility of each e-mail user to ensure e-mail communication is used appropriately. Users shall not use e-mail to harass, offend, or annoy others or send communications that are not appropriate for a professional business environment. Misuse of computing, networking, or automated information resources may result in loss of computing privileges and may be cause for prosecution under applicable state or federal statutes and/or disciplinary action.

b. Chain of Command Observed. The same protocol observed in telephone contacts shall be applied to e-mail contacts. Users shall not send e-mail messages

to anyone they would not normally call directly on the telephone.

c. Confidential and Sensitive Information. Users shall not use e-mail to send or receive unencrypted confidential or sensitive information. These types of messages are vulnerable to unauthorized access.

(1) Confidential Information. Refers to information that must remain private and protected. This information is not generally known to the public and is required to keep protected from disclosure. It includes financial information, health records, personal identifiers, employee information, contracts, and agreements.

(2) Sensitive Information. Refers to information that must be protected due to its nature and the potential harm it could cause if disclosed inappropriately. It includes personal identifiers, financial information, health records, and any other information that could lead to identity theft or discrimination.

(3) Information obtained in the California Law Enforcement Telecommunications System shall not be included in or attached to any e-mail messages.

d. E-Mail Forwarding. E-mail messages sent outside the Department's internal network are not protected by CHP network security. For this reason, users shall not create e-mail rules to automatically forward e-mail messages to personal e-mail accounts.

(1) Users shall not create e-mail rules to automatically delete any departmental messaging for security-related purposes. This includes e-mails from the Information Security Office (ISO) and the Information Technology Support Unit.

e. Third-Party Internet E-Mail Providers. Departmental users shall not access third-party Internet e-mail providers, including, but not limited to, Gmail, Hotmail, Yahoo, and America Online from CHP network computers.

f. Privacy. The CHP e-mail system is not private. The Department has the right to monitor and log all network activity, including e-mail activity, with or without notice. Users should have no expectations of privacy when using these resources.

g. Standard Operating Procedures. Commanders shall ensure appropriate policies and procedures for the use of e-mail are incorporated into their command's Standard Operating Procedures.

h. Inappropriate Solicitation. The Department's e-mail system may not be used as a method to solicit donations for, or participation in, charity events other than

those which are departmentally sponsored and supported. Examples of sanctioned events include Our Promise: California State Employees Charitable Campaign, United States Savings Bond drive, blood drives, and food drives. E-mail solicitation not meeting these criteria must be approved by the commander responsible for the immediate Area(s) or section(s) subject to the solicitation. As such, if an e-mail is directed Areawide, the affected Area commander will serve as the approving authority. If the e-mail is directed Division-wide, the Division commander will serve as the approving authority. Approval by the appropriate Commissioner is required for Department-wide solicitations.

i. Notification. Commanders shall ensure the following:

(1) All users are made aware of policy and procedures regarding e-mail use as outlined in this manual.

(2) A current CHP 101, Appropriate Use of Automated Information & Systems Statement, is on file for all employees.

(3) A CHP 101A, Agreement With Outside Entities to Establish Remote Access Privileges to CHP Automated Computer Systems and Information, is on file for nonemployees (e.g., contractors) who have been granted access to departmental computer resources.

j. Outdated Messages. It is the responsibility of each user to monitor and maintain all e-mail messages sent and received through their own account. On a regular basis, each user should:

(1) Review and manage their mailbox.

(2) Delete all messages that are not part of a business record.

NOTE: Once messages in the “Deleted Items” folder are deleted, they will be recoverable for up to 30 days, but messages are unrecoverable thereafter.

k. E-Mail Retention.

(1) E-mail Folders:

(a) Inbox and Drafts Items. Messages stored within the “Inbox” and “Drafts” folders are retained for one year.

(b) Sent Items. Messages stored within the “Sent Items” folder are retained for two years.

(c) Deleted Items and Junk Email. Messages in Deleted Items and “Junk

Email" folders are retained for 30 days.

(d) Subfolders. Messages stored within subfolders follow the retention of the parent folder.

(e) Archive. Messages stored in the "Archive" folder are retained for five years.

1 Legacy Archived Messages. The CHP has discontinued support of messages that are archived to the local personal computer (C: drive); if lost, archived messages are unrecoverable.

(2) Instant Message Communications. Individual and group instant messaging (e.g., Microsoft Teams, Mobile Digital Computer) are retained for three days.

(3) Exemptions. Exemption requests must be submitted through the chain of command to Information Management Division (IMD). The IMD will obtain approval from the Office of the Commissioner.

3. REPORTING MISUSE OF E-MAIL.

a. If misuse of the departmental e-mail system is discovered, the commander or their designees shall be notified. Commanders or their designees shall contact Computer Crimes Investigation Unit (CCIU). While CCIU can provide technical support and answer technical questions, it is the responsibility of the respective commander to ensure a thorough and comprehensive audit of the e-mail account in question is performed, and that an internal investigation is conducted (if appropriate) in accordance with HPM 10.2, Internal Investigations Manual.

b. A user who receives excessive, inappropriate, and/or nonbusiness-related e-mail through the departmental e-mail system shall immediately send the e-mail as an attachment to their commander for investigation and resolution, then delete the e-mail from their account. Commanders who are notified of the receipt of an excessive, inappropriate, and/or nonbusiness-related e-mail shall accomplish one of the following, if the sender is:

(1) A departmental employee assigned to the command of the receiver of the e-mail, initiate an investigation in accordance with HPM 10.2.

(2) A departmental employee assigned to a command other than the command of the receiver of the e-mail, notify the sender's commander, who shall initiate an investigation in accordance with HPM 10.2.

(3) Not a departmental employee, transmit a message to the sender informing them their message is classified as excessive, inappropriate, and/or nonbusiness-related and request they cease sending such e-mails to the departmental employee. If nondepartmental employees continue to send such e-mail messages to departmental employees, commanders should contact their Division Administrator who can assist, or coordinate with the Information Technology Support Unit to block or filter e-mail messages from e-mail addresses.

c. The IQAP relates to inappropriate use of the Department's e-mail system only. Issues regarding the monitoring and/or misuse of the Internet should immediately be directed to the Internal Affairs Section.

d. Phishing, or potentially malicious, e-mail may be reported to the ISO by clicking the "Phish Alert Report" button. Users may then delete the message from their inbox if not already deleted. The ISO will contact the user if additional information is needed or to provide direction.

THIS PAGE INTENTIONALLY LEFT BLANK