CHAPTER 3

E-MAIL

REVISED OCTOBER 2023

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3

E-MAIL

1. GENERAL.

   a. E-mail System Defined. An e-mail system allows computer users the ability to type a message at one computer or terminal and send the message to a user at another computer or terminal. The system stores the message until the receiver chooses to read it.

   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, and to identify users who are sending and receiving excessive, inappropriate, and nonbusiness-related e-mail.

   d. California Public Records Act Requests. All requests for e-mail records, under Government Code Section 6250, Inspection of Public Records, 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.

2. POLICY.

   a. For Business Use Only. California Highway Patrol 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. Computer 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. Per Executive Order S-03-10, agencies under the Governor's authority shall transition to the state's shared e-mail solution. In compliance with this order, the CHP's e-mail will be managed by the current state-awarded service provider. Confidentiality, integrity, and availability of the e-mail system are dependent on the service provider. Computer users shall not use the CHP's internal e-mail or Internet e-mail to send or receive unencrypted confidential or sensitive information. These types of messages are vulnerable to hacker interception, viewing, monitoring, and reading.

(1) No information obtained in the California Law Enforcement Telecommunications System shall 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 their e-mail messages to personal e-mail accounts.

e. Third-Party Internet E-Mail Providers. Departmental users shall not access third-party Internet e-mail providers such as 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. E-mail messages, even those that have been deleted from the "Deleted Items" folder, can be recovered for up to 30 days from the date of deletion and may be used in any subsequent investigative processes. E-mail messages in user mailboxes placed on Legal Hold are recoverable until the Legal Hold is expired or removed.

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 the United California State Employees 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 may approve it.

Approval by the appropriate Commissioner is required for Departmentwide solicitations.

i. Notification. Commanders shall ensure the following:

(1) All departmental users are made aware of policy and procedures regarding e-mail and Internet 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 (i.e., 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, the messages will be recoverable for up to 30 days. Thereafter, messages are unrecoverable.

k. Archive Messages. Messages are archived to the local personal computer (C:\ drive) and are not backed up. If lost, archived messages are unrecoverable.

l. E-mail Retention.

(1) E-mail folders:

(a) Inbox, Drafts, and Sent Items. Messages stored within the Inbox, Drafts, and Sent Items folders, including nested folders, are retained for one year.

(b) Subfolders. Messages stored within subfolders, including nested folders, are retained for two years.

(c) Deleted Items and Junk Email. Messages in Deleted Items and Junk Email folders, including nested folders, are retained for 30 days.

(d) Archive. Messages stored in the Archive folder, including nested folders, are retained for five years.

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

(3) Exemptions. Exemption request must be submitted through the chain of command to the 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 initially discovered at the command level, commanders or their designee shall contact the Computer Crimes Investigation Unit (CCIU) to obtain access to the e-mail account in question. While the 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 an inappropriate e-mail through the departmental e-mail system shall immediately forward the e-mail to their respective commander for investigation and resolution. After forwarding an inappropriate e-mail, the user shall delete the e-mail from their respective account. Commanders who are notified of the receipt of inappropriate e-mail shall accomplish one of the following, if the sender of the inappropriate e-mail 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 inappropriate and request they cease sending inappropriate e-mail to the departmental employee. If nondepartmental employees continue to send inappropriate e-mail messages to departmental employees, commanders should contact their Division Network Administrator who can assist, or coordinate with, the Customer Support Cybersecurity Section (CSCS) to block or filter e-mail messages from specific 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 Department's Office of Internal Affairs.

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

THIS PAGE INTENTIONALLY LEFT BLANK.