CHAPTER 18

ACCEPTABLE USE POLICY

REVISED FEBRUARY 2025

TABLE OF CONTENTS

INTRODUCTION 18-3
SCOPE 18-3
POLICY 18-3
Acceptable Activities 18-3
Unacceptable Activities 18-3
CHP E-Mail Messages and Instant Messages 18-5
External E-Mail and Instant Message Services 18-5
File Sharing 18-5
Generative Artificial Intelligence 18-6
ENFORCEMENT 18-6

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 18

ACCEPTABLE USE POLICY

1. INTRODUCTION. The CHP expects responsible, effective, and lawful use of the CHP network, computer systems, the Internet, and other technology resources such as e-mail and telephones to achieve the Department's business goals and mission. These resources are provided to conduct state business and are routinely monitored for improper use. Anyone using these resources expressly consents to such monitoring.

a. Anyone granted access to CHP technology resources is required to read and agree to abide by the CHP Acceptable Use Policy.

2. SCOPE. This policy applies to anyone, including but not limited to employees, contractors, consultants, temporary employees, volunteers, and allied agencies having access to or use of technology resources owned, operated, or managed by CHP or the State of California. This policy applies to the use of CHP technology resources from remote locations (e.g., while telecommuting) as well as from a CHP worksite.

3. POLICY.

a. Acceptable Activities.

(1) Acceptable activities are those in accordance with the laws and policies of the United States Government and the State of California; are consistent with the purpose, goals, and mission of the CHP; and are appropriate to each user's assigned job duties and responsibilities.

(2) The following list provides examples of acceptable activities:

(a) Research to enhance compliance and law enforcement program activities.

(b) Communications for business and administrative purposes.

(c) Incidental, necessary communications pertaining to personal and family matters, such as a telephone call or e-mail to a child's daycare or school.

b. Unacceptable Activities.

(1) The following list provides examples of unacceptable activities:

(a) Engaging in any activity that is illegal under local, state, federal, or international law while utilizing CHP owned resources.

(b) Use for outside employment, business, or personal gain.

(c) Use for any illegal, discriminatory, or defamatory purpose including the transmission of threatening, obscene, or harassing messages.

(d) Activities that interfere with an employee's ability to perform their job duties or responsibilities.

(e) Browsing inappropriate websites such as those that contain nudity or sexual content, malicious content, or gambling activities.

(f) Intentionally attempting to access information resources without authorization and/or a business need.

(g) Use of any software, including free web-based software, that has not been approved by the Information Security Officer (ISO) and/or Chief Information Officer (CIO) via the software evaluation process as described in Highway Patrol Manual, 40.4, Information Security and Administration Manual, Chapter 10, Software.

(h) Installing or connecting unauthorized software or hardware on CHP owned and/or managed information systems.

(i) Storing personal or nonbusiness-related data and multi-media files on CHP servers or other centrally managed resources.

(j) Revealing account passwords to others or allowing use of accounts by others. This includes family and other household members when teleworking.

(k) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account the employee is not expressly authorized to access, unless these duties are within the scope of the employee's regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

(l) Network scanning (e.g., Internet Protocol, port) or security scanning is expressly prohibited unless authorized by the ISO.

(m) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is part of the employee's regular duties.

(n) Circumventing user authentication or security of any host, network, or account.

c. CHP E-Mail Messages and Instant Messages.

(1) E-mail messages and instant messages (IM) distributed via CHP e-mail and IM systems are CHP property and not the private property of individual users.

(2) The CHP e-mail and IM systems must not be used for:

(a) Automatic forwarding of e-mail messages to external recipients.

(b) Transmitting confidential information to external recipients unless encrypted with a method approved by the ISO and appropriate to the employee's job duties and responsibilities.

(c) Circulating chain mail, jokes of the day, nonbusiness-related video clips, and digital images

(d) Distributing religious, political, sexual, or offensive content.

d. External E-Mail and Instant Message Services.

(1) While connected to the CHP network, use of external e-mail and IM services (e.g., personal e-mail and IM accounts) is prohibited unless expressly approved by the ISO.

e. File Sharing.

(1) State and federal law prohibits the unauthorized transfer or sharing of music, movies, software, and other intellectual property. Therefore, unauthorized use of peer-to-peer (file sharing) software is prohibited. Other technologies such as File Transfer Protocol must be approved by the ISO for business use.

f. Generative Artificial Intelligence.

(1) Requests for the use of Generative Artificial Intelligence (GenAI) will be evaluated and approved on a case-by-case basis via the software evaluation process. Refer to HPM 40.4, Chapter 10, for details regarding this process.

(2) Should a request for the use of GenAI be approved, users will be required to sign a GenAI Acceptable Use Memorandum of Expectations (MOE), which will be provided with Information Management Division's approval memorandum, prior to access being granted or beginning use. The MOE will contain acceptable use terms and conditions for both the use of the software and the approved use case, as required by the ISO, CIO, Agency Information Officer, and/or the California Department of Technology, upon review and approval of the SIMM 5305-F, Generative Artificial Intelligence Risk Assessment. The Software Management Program Manager and Privacy and Risk Management Administrator will work with the requestor during the software evaluation process to document the requested use case parameters for inclusion in the MOE.

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