CHAPTER 23

ONEDRIVE AND SHAREPOINT

REVISED NOVEMBER 2025

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 23

ONEDRIVE AND SHAREPOINT

1. PURPOSE. The purpose of this policy is to establish a standard for the CHP OneDrive and SharePoint as cloud services and file storage solutions.

2. SCOPE. This policy is applicable to all CHP employees and nondepartmental users, such as contractors and consultants. This includes users authorized to utilize CHP resources while using a departmentally or personally owned computer or workstation, regardless of whether it is connected to the CHP network.

3. GENERAL. The CHP expects responsible, effective, and lawful use of OneDrive and SharePoint 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 OneDrive and/or SharePoint expressly consents to such monitoring.

4. POLICY. OneDrive provides CHP users the ability to share files and folders with internal users for collaboration and cooperation. SharePoint shall be used for external sharing. Command approval is required for CHP employees to share externally, and guest accounts are required for recipients in SharePoint. To request a guest account and approval to share externally, a ServiceNow request must be submitted. If a requested recipient is not a member of a law enforcement agency or State of California Department or agency, CHP Information Security Officer approval is required before the guest account can be created.

a. For Business Use Only. OneDrive and SharePoint may be used in accordance with the CHP acceptable use policy. OneDrive is not a location to store departmental files, as OneDrive is connected to the user's account. The user's OneDrive is deleted with their account upon separation from the Department, including shared files. SharePoint may be used to store departmental files. Each employee should consider the use of OneDrive and SharePoint a privilege and shall use these resources for business purposes only. Please refer to Chapter 18, Acceptable Use Policy, of this manual for additional information.

b. OneDrive and SharePoint may be used to store a user's own Personally Identifiable Information (PII) and Payment Card Industry (PCI) data. Both PII and PCI data, if accessed by unauthorized entities, could cause personal or institutional financial loss or constitute a violation of statute, act, or law. Examples of PII and PCI data may include, but are not limited to, the following:

(1) Social security numbers.

(2) Bank account or credit card numbers.

(3) Data protected by the Health Insurance Portability and Accountability Act.

(4) Login and/or password credentials.

c. Data stored in OneDrive may not be shared with any outside entity. Data loss prevention policies are in place to enforce this restriction. Only authorized CHP employees can share PII and PCI data outside the CHP network.

d. Requests to increase OneDrive storage space will not be approved. Each user is responsible for managing their allocated space.

e. Privacy. There shall be no expectation of privacy while using OneDrive and/or SharePoint for daily business operations. The CHP reserves the right to inspect, monitor, and review all OneDrive and SharePoint resources including files, data, and e-mail records without the consent of the holder of such records.

f. Security. OneDrive and SharePoint are secure systems. Information security is a vital concern of the Department. All provisions outlined in this manual relating to confidential information remain in effect when using OneDrive and/or SharePoint. It is each employee's responsibility to maintain confidentiality of departmental documents and to ensure only persons designated to receive such information are the actual recipients.

(1) Files shall only be shared with others who are authorized to obtain such content.

(2) OneDrive and SharePoint shall not be used to distribute unauthorized, restricted, or personal content including, but not limited to personal music, videos, photos, or software.

(3) The policy requirements of this manual, including Chapter 17, Use of Personal Smartphones and/or Tablets to Access State Electronic Mail, and Chapter 18, apply to the use of OneDrive and SharePoint.

g. California Law Enforcement Telecommunications System. Employees of the CHP shall not use non-CHP approved cloud service providers, including, but not limited to Microsoft OneDrive, to store California Law Enforcement Telecommunications System derived data or Criminal Justice Information Services data.

5. ACCESS. All employees who have an Active Directory account established and have completed the CHP-implemented Multi-Factor Authentication (MFA) process have access to OneDrive and SharePoint externally. Any external guest user that has been provided authorized access to SharePoint files is required to use MFA. If further assistance is needed, users may contact the Information Technology Support Unit at (916) 843-3899, or submit a work order via ServiceNow.

a. OneDrive and SharePoint are compatible with updated industry standard web browsers. It is each employee's responsibility to ensure the appropriate computer equipment and web browser software are used and to provide a compatible Internet service provider, including payment for any communication costs, when using these systems remotely.

b. Accountability. The CHP shall control individual employee and nondepartmental user access to departmental computer and/or information systems resources. All users shall be aware of the systems and files they access or share.

c. Employee and Nondepartmental User Responsibility.

(1) Pursuant to policy established in this manual, CHP employees and nondepartmental users are responsible for protecting the Department's information technology assets and data. This includes ensuring the security and privacy of any CHP data that is shared both internally and externally.

(2) All users shall report any lost or stolen computer or device to their commander as soon as possible (refer to Highway Patrol Manual [HPM] 11.2, Materials Management Manual, Chapter 8, Equipment). Commanders shall notify Information Management Division within five business days.

(3) Employees shall be aware of with whom CHP data is being shared. All users, including nondepartmental users, shall be made aware of the responsibility of ensuring CHP data will only be accessed and/or viewed by individuals with both a right to know and a need to know. Any other access is prohibited.

6. ENFORCEMENT. Any employee or nondepartmental user found to have violated this policy is subject to disciplinary action. Misuse of computing, networking, or information systems resources may result in loss of computing privileges and may be cause for disciplinary action and/or prosecution under applicable state or federal statutes.

a. Reporting Misuse of California Highway Patrol OneDrive and/or SharePoint. Misuse of OneDrive and/or SharePoint discovered by the Department's Computer Crimes Investigation Unit (CCIU) will be reported through channels to the appropriate commander for investigation and resolution.

(1) If misuse of OneDrive and/or SharePoint is discovered initially at the command level, commanders, or their designee, shall contact CCIU to obtain access to OneDrive account or SharePoint in question. The CCIU can provide technical support and answer technical questions. However, it is the responsibility of the respective commander to ensure a thorough and comprehensive audit of the account in question is performed, and an internal investigation is conducted (if appropriate) in accordance with HPM 10.2, Internal Investigations Manual.

(2) Employees who receive inappropriate, malicious, or compromising files through OneDrive or SharePoint shall immediately notify their respective supervisor and/or commander for investigation and resolution.

ANNEX A

DEFINITIONS AND TERMS

a. Account. A series of rights or permissions granted to an individual that permits access to a network and/or information system.

b. Computer and/or Information Systems Resources. A computer or computing system and/or application used to complete job-related tasks efficiently.

c. E-Mail. A method of communication that allows computer users the ability to send a message from one computer or workstation to another.

d. External User. Individuals who are nondepartmental users and are required to have a CHP guest account created.

e. Internal User. CHP employees or nondepartmental users that have been provided CHP login credentials.

f. Nondepartmental User. Includes contractors, consultants, explorers, retired annuitants, senior volunteers, student assistants, vendors, or any individual not under the direct employment of the CHP.

g. OneDrive. A Microsoft-based cloud service file share solution.

h. Trusted Device. A departmentally owned computing device managed by the CHP, or a departmentally owned cell phone enrolled into the CHP's mobile device management system.

i. Web Browser. A software application for connecting to and viewing information and resources on the World Wide Web, also referred to as the Internet.

THIS PAGE INTENTIONALLY LEFT BLANK