CHAPTER 17

USE OF PERSONAL SMARTPHONES AND/OR TABLETS TO ACCESS STATE ELECTRONIC MAIL

REVISED JUNE 2017

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 17

USE OF PERSONAL SMARTPHONES AND/OR TABLETS TO ACCESS STATE ELECTRONIC MAIL

1. PURPOSE.

a. The California Highway Patrol (CHP) has an obligation to the people of the State of California to protect the sensitive or confidential information it collects, maintains, or processes. The use of personal smart phones and/or tablets to access state e-mail provides convenient access for employees with a business need and reduces expenses for the Department. However, the use of personal smartphones and/or tablets for this purpose introduces an increased level of risk to CHP information. This policy addresses the requirements needed to obtain access to Department e-mail from personal smartphones and/or tablets.

2. RISKS.

a. Unlike state information assets, personal smartphones and/or tablets are not managed by state information technology (IT) administrators specifically dedicated to performing the necessary maintenance and ensuring the protection of the device or information stored on the device. If security precautions are not taken and maintained, sensitive or confidential information may be compromised. An example would be if the personal smartphone and/or tablet, which is not encrypted or password protected, is lost, stolen, or in some way made available to unauthorized individuals. Additionally, with the comingling of departmental information with an employee's personal information, work-related information must be made available in the case of a litigation hold, e-discovery, public disclosure, or audit processes.

3. POLICY.

a. The use of a personal smartphone and/or tablet to access state e-mail is subject to all state and Department policies and standards, including the Statewide Information Management Manual (SIMM) 5360-A, Telework and Remote Access Security Standard, and shall be consistent with the Statewide Enterprise Architecture.

b. Employees authorized to use personal smartphones and/or tablets to access state e-mail must agree to protect state information from unauthorized access and use by others, including family members and friends, and ensure the smartphone and/or tablet is secured when it is unattended (i.e., locked in a cabinet or drawer, secured in locked rooms within secured buildings, and not left in unattended vehicles or other locations where it may be easily stolen). Employees shall also

use and securely maintain (i.e., not written down or shared) “strong” passwords for all information assets, including smartphones and/or tablets, which are capable of restricting access by using a password.

c. Information Management Division (IMD) shall ensure control requirements applied to the use of smartphones and/or tablets, of both state-owned and personally owned information assets, are in place before connections to the state IT infrastructure are allowed.

4. PROCEDURES.

a. Approval Process. Employees wishing to use personal smartphones and/or tablets to access state e-mail shall do the following:

(1) Submit a complete CHP 109, Information Technology Request, through their chain of command to IMD. Commanders shall confirm that a valid business need for the access exists. The use of smartphones and/or tablets, as well as other personal mobile computing devices, must be authorized by the Division commander, Department Information Security Officer, and IMD.

(2) Submit a SIMM 5360-B, Remote Access Agreement (available on the CHP Intranet site, under Forms, Other), to IMD in lieu of a Telework Arrangement when smartphone and/or tablet use and other mobile computing implementations do not fall within the definition of a flexible or regular Telework Arrangement (refer to Chapter 11, Remote Computing, Annex A, of this manual). The completed and signed SIMM 5360-B shall be kept in the employee’s personnel file and reinstated every three years.

(a) The following are conditions from the SIMM 5360-B (refer to Annex A of this chapter) that must be agreed and adhered to by the employee, supervisor/manager, and commander before allowing the use of a personal smartphone to access state resources such as e-mail:

1 Maintain established security controls, such as strong passwords, device and data encryption, inactivity time-out lock, and automatic updates.

2 Electronically register device information.

3 No alteration, disabling, or circumvention of established security controls.

4 Maintain back-ups in accordance with authorized agency procedures.

5 Allow IT administrators to define, manage, and validate device security controls.

6 Provide IT administrators the ability to issue remote data wipe and device kill commands in order to protect the confidentiality of state data residing on the device.

7 Immediately report the loss, theft, or damage of the device.

b. Requirements and Conditions.

(1) Telework users who require assistance in making the configuration changes necessary to meet these requirements for their personal computing assets may need to seek the assistance of professional computer support/repair services at their own expense.

(2) Employees wishing to use personal smartphones and/or tablets to access CHP e-mail shall complete the Information Security and Privacy Protection training course located on the CHP Intranet site (under Training, Online Training), prior to connecting to CHP e-mail.

(3) Personal smartphone devices must have the ability and be configured to use the following security features:

(a) Hardware or software encryption for state information on the device.

(b) Data encryption in transit (Secure Socket Layer).

(c) Remote lock and wipe/delete capabilities.

(e) Must be able to receive up-to-date operating system and software patches.

(f) Must be compatible with the Microsoft Office 365 e-mail service CHP has adopted as its e-mail service provider.

THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX A

SIMM 5360-B, REMOTE ACCESS AGREEMENT

Employee Name:		Office/Branch:	
Employee Telephone:		Employee Email Address:	
Supervisor/Manager Name:		Supervisor/ Manager Email Address:	
Supervisor/Manager Telephone:			

This agreement is to be used in lieu of a Telework Agreement when an employee is authorized to establish a remote access connection to IT infrastructure for work-related functions which fall outside the realm of a traditional telework arrangement, such as use of a smart phone or other mobile computing device which establishes a remote access connection to state IT infrastructure. As with any casual or formal telework arrangement, the employee, Supervisor/Manager and Office Chief are to acknowledge they have read, understand and agree to adhere to all applicable state policies, standards and procedures including, but not limited to the agency's Acceptable Use Policy, the Telework and Remote Access Security Standards (SIMM 5360-A) and applicable provisions of the Telework Program Policy and Procedures. Applicable provisions of the Telework and Remote Access Security Standard and Telework Program Policy and Procedures include but are not limited to the following:

- Maintaining established security controls, such as strong passwords, two-factor authentication, device and data encryption, antivirus and antispyware software, personal firewalls, content filtering software and automatic updates;
- Electronic registration of device information;
- Disabling of non-essential functions and services on the device;
- Not altering, disabling or circumventing established security controls;
- Maintaining back-ups, only in accordance with authorized state entity procedures;
- Allowing IT Administrators to define, manage and validate device security controls;
- Providing IT Administrators the ability to issue remote data wipe and device kill commands in order to protect the confidentiality of state data residing on the device, and;
- Immediately reporting the loss, theft or damage of the device.

The following assets are authorized and will be used to make remote connections:

Make	Model	Asset Identification

The following state information systems will be accessed remotely with the above referenced assets:

I have read, understand and acknowledge the state entity Telework Program Policy and Procedure and state Telework and Remote Access Security Standard. I also understand that when my use of any personal computing equipment is authorized by the state entity for remote access purposes, this use may result in a lack of privacy related to those items.

Employee Signature:		Date:	
Supervisor/Manager Signature:		Date:	
Office Chief Signature:		Date:	