CHAPTER 11

REMOTE COMPUTING

REVISED DECEMBER 2025

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 11

REMOTE COMPUTING

1. PURPOSE. The purpose of this policy is to define standards for connecting to the CHP's network from any computing device outside of the Department's internal network. These standards are designed to minimize the potential risk to the CHP from damages which may result from unauthorized or inappropriate use of CHP resources. Damages include but are not limited to: the loss of sensitive or confidential data and intellectual property, and damage to CHP's public image and critical CHP internal systems.

2. DEFINITIONS.

a. Computing Device. Any device with computing capacity similar to a computer (e.g., computers, laptops, or tablets; Apple or Android devices).

b. Information Assets. All categories of information (confidential, personal, sensitive, or public); all forms of information assets (paper or electronic); and information technology (IT) facilities, equipment, and software owned or leased by state agencies. (Refer to State Administrative Manual [SAM], Section 5300.4, Definitions.)

c. Information Technology Administrators. The Department's IT staff who are responsible for the support and security of the IT infrastructure.

d. Information Technology Infrastructure. An agency's IT platform for the support of departmental programs and management, including equipment, software, and communication networks. (Refer to SAM Section 4989.1, Definition of Desktop and Mobile Computing.)

e. Mobile Digital Computer. Portable computing devices designated for field units that are linked to the Computer-Aided Dispatch environment.

f. Multihomed Host. A host connected to two or more networks. For example, a computer may be connected to a serial line and a Local Area Network (LAN) or to multiple LANs. Only in rare situations are multihomed computers appropriate, and in most situations, a multihomed computer can become a security risk. Departmental employees shall not multihome their computing devices.

g. Multifactor Authentication. The use of multiple factors to determine a user's identity. Common factors of authentication include "something you know"

(password), “something you have” (token or key), or “something you are” (biometric).

h. Remote Access. The connection of an information asset from an off-site location to an information asset on state IT infrastructure.

i. Security Baseline. An analysis of a computing device to determine its current security posture. A security baseline is a composite of attributes consisting of antivirus status, software patching status, and security settings.

j. Split Tunneling. The process of allowing a remote virtual private network (VPN) user to access a public network, most commonly the Internet, at the same time the user is allowed to access resources on the VPN. A disadvantage of this method is it essentially renders the VPN vulnerable to attack as it is accessible through the public, nonsecure network. (Refer to paragraph 2.n. of this chapter.)

k. Telework. An arrangement in which an employee regularly performs officially assigned duties at home or an alternate work site.

l. Tunneling Architecture. A high-level remote access architecture that provides a secure tunnel between a telework device and a tunneling server through which application traffic may pass. Tunnels use cryptography to protect the confidentiality and integrity of the transmitted information between the client device and the VPN gateway.

m. Two-Factor Authentication. Authentication based on two factors of identification. (Refer to paragraph 2.g. of this chapter.)

n. Virtual Private Network. A virtual network, built on top of existing physical networks, that provides a secure communication tunnel for data and other information transmitted between networks.

o. Web-Based Connection. Provides access to one or more applications through a single, centralized interface through direct application access or portal architecture (typically a web browser to a portal server located within the demilitarized zone). This type of connection creates an area that serves as a boundary between two or more networks and isolates the information asset from the internal private network.

3. SCOPE.

a. This policy applies to all CHP employees, contractors, vendors, and agents using either a CHP-owned or personally owned computer or computing device used to connect to the CHP network or CHP network resource from a remote location.

This policy applies to remote access connections used to do work on behalf of the CHP, including reading or sending e-mail and viewing CHP Intranet site resources.

b. Remote access covered by this policy includes, but is not limited to, departmental web e-mail, web-based applications, portal applications, remote desktop architecture, VPN, Secure Shell, remote proxy, or any other method used to access CHP IT resources from a non-CHP network location using either personal or departmental computing devices.

4. GENERAL POLICY. Pursuant to Section 11549.3 of the Government Code, CHP must be in compliance with Statewide Information Management Manual (SIMM) 5360-A, Telework and Remote Access Security Standard. The following policies and procedures coincide with SIMM 5360-A; however, it is the responsibility of all users to read and comply with all the requirements set forth in SIMM 5360-A.

a. Revocation of Rights. All remote access privileges are granted in good faith that users will proactively maintain a secure computing environment. Privileges may be revoked temporarily or permanently at the discretion of the Information Management Division (IMD) and the Technology Infrastructure Section (TIS). Additionally, commanders may request a user's permissions to be revoked by submitting a ServiceNow request. It is the responsibility of the user's commander to inform the user of the loss of their privileges.

b. Risk Management. All network access will undergo a risk assessment utilizing the Department's security tools. Depending on the level of risk, the Department may require additional factors of authentication or disallow access altogether. Indicators of risk factors may include the following:

(1) Status of the computer accessing resources.

(2) Status of the user account accessing resources.

(3) Antivirus status of the computer accessing resources.

(4) Source network and location of the computer accessing resources.

(5) Current CHP network security posture and health.

c. Advanced Authentication. All remote access services are subject to requirements of an advanced authentication system which will require the user to use multifactor authentication. Some services may use different solutions. See Chapter 19, Mobile Digital Computer Oversight and Use, of this manual, for policy regarding the use of advanced authentication for Mobile Digital Computer laptops.

5. E-MAIL WEB ACCESS.

a. Background. E-mail web access permits authorized users to access their departmental e-mail accounts using a web browser. E-mail web access offers users greater flexibility and increased mobile access. This access requires no special software applications or extra licensing, provides cost savings to the Department, and allows users to access their departmental e-mail accounts via any computer with an Internet connection. Additionally, e-mail web access provides improved auditing and tracking capabilities.

b. Authorization. All users granted a departmental e-mail address are granted limited authorization to use e-mail remotely.

NOTE: Authorized users may use departmental e-mail only in the course of conducting business for the State of California, including business with the federal government and any city, county, or other public agency.

c. Requirements for Use. It is a user's responsibility to provide the appropriate computer equipment, browser software, and the necessary internet service provider (ISP), including any personal communication costs. The Department will not pay for the computer equipment, ISP, or toll charges that may be incurred while using e-mail web access. The Internet browser being used must support the latest encryption technology. The computer must also have up-to-date antivirus detections. Internet browsers and antivirus software unable to meet the minimum specifications will be denied access. Minimum specifications are updated regularly, and users may reach out to the IT Support Unit to obtain the current minimum specifications.

6. VIRTUAL PRIVATE NETWORK.

a. Background. The Department provides VPN services for CHP-owned computer equipment. Users are required to have authorization before obtaining these services.

b. Authorization. Authorization for VPN use shall be obtained by submitting a ServiceNow Access Request and using the Request for VPN access form. The request must be submitted by the user's supervisor and must include the user's manager's approval.

c. Requirements for Use. The following criteria must be met to use VPN services:

(1) Only CHP-owned and managed computers may use the Department's VPN services.

(2) Computers failing to meet the Department's security baseline may have VPN access restricted until the computer has been remediated.

(3) **Users must use multifactor authentication**.

7. TELEWORK POLICY.

a. Responsibilities.

(1) Managers/Supervisors.

(a) Before managers and/or supervisors authorize work to be performed under an STD. 200, Telework Agreement, they are responsible for ensuring the following IT and information security policies are followed:

1 Provide employee training on the use of equipment and software as required for teleworkers to function effectively and independently.

2 Ensure all software installed for the telework option is in accordance with software copyright laws and compatible with policies in this manual, software standards, and SIMM 5360-A.

3 Ensure compliance with policies in this manual and SIMM 5360-A in order to protect the CHP's assets when accessing, storing, or transporting CHP's information.

4 Report security incidents immediately when they occur.

(2) Employees. Employees interested in teleworking must:

(a) Understand the requirements contained in Highway Patrol Manual (HPM) 10.3, Personnel Transactions Manual, Chapter 46, Teleworking, and SIMM 5360-A.

(b) Abide by the provisions set forth in HPM 10.3, Chapter 46, state information security policies, and SIMM 5360-A.

(c) Establish and maintain a work area that is clean, safe, and free from hazards.

(d) Maintain CHP-owned and/or personally owned equipment, devices, and services associated with achieving a safe, secure, and healthful telework environment as identified in SIMM 5360-A.

(e) Report security incidents immediately to their supervisor.

(f) Repair and/or replace any damaged, lost, or stolen CHP-owned equipment assigned to the teleworker if the damage, loss, or theft is determined by management to be due to gross negligence on the part of the employee. (Procedures for reporting lost, stolen, or destroyed property or equipment are provided in SAM, Chapter 8600, Property Accounting, and Section 8643, Accounting for Property Disposition - Lost, Stolen, or Destroyed Property).

(g) Comply with all applicable policies, standards, procedures, and guidelines.

(h) Ensure their remote access connection is given the same consideration as the employee's on-site connection to the CHP network.

(i) Ensure unauthorized users are not allowed access to CHP internal networks through their VPN connections.

(j) Ensure only authorized individuals can view information obtained by the VPN connection.

(k) Ensure all computers connected to CHP internal networks via their VPN are running a CHP-approved operating system, up-to-date operating system/software patches, and antivirus definitions.

(l) Ensure VPN clients are installed solely on CHP-owned equipment. Employees must use a CHP computing device to establish a VPN connection.

(m) Ensure computers used to connect through the CHP VPN are not used for general Internet access outside of the CHP network. Using an Internet browser (such as Edge, Mozilla Firefox, Safari, or Google Chrome) to directly access web resources through a home network, Internet hotspot, or hotel network, for example, exposes the computer to malware which may then be introduced into the CHP network when the computer is subsequently connected via VPN.

(n) Limit a VPN session to a maximum connection time of eight hours. Logging off and then immediately logging back on is permitted as often as needed to complete CHP business.

(o) **Ensure all computing equipment connected to the CHP network for telework purposes are CHP-owned information assets which shall be configured in accordance with secure enterprise and agency standard configurations**, including those set forth herein. Teleworking employees shall not connect personally owned information assets to the

state IT infrastructure at the network level unless an approved written exception applies and is implemented in accordance with the additional use of personally owned information assets standards herein.

(p) Only connect to state IT infrastructure through secure encrypted channels authorized by IMD. These channels may include encrypted VPN, encrypted web access, encrypted broadband, and encrypted dial-up connections. At no time may the teleworking employee initiate two simultaneous connections to different networks (e.g., no split tunneling or multihomed connection). Just as in an Area or Division office, security measures cover not only information systems and technology, but all aspects of the information and information systems used by the employee, including paper files, other media, storage devices, and telecommunications equipment (e.g., laptops and tablets) used in the course of work. Employees must keep government property and information safe, secure, and separated from their personal property and information.

(q) Adhere to all other information security policies, standards, and procedures regarding the use of state information assets, regardless of the work location. Teleworking employees shall not disable, alter, or circumvent established security controls on state information assets used to connect to state IT infrastructure, such as antivirus software, antispyware software, firewalls, content filtering software, and automatic software updates.

(r) Comply with tax laws.

NOTE: The CHP is not responsible for substantiating an employee's claim of tax deductions for operating an office in the employee's home. An employee should seek advice from a tax advisor concerning in-home office deductions.

(s) Complete the required Information Security Privacy Protection training located on the CHP Intranet site under Training ➢ Online Training. Once all assigned modules are completed, the employee shall certify the training by forwarding their confirmation e-mail to their Employee Training Records System (ETRS) Coordinator. The e-mail shall be retained in the employee's personnel training file. The command's training coordinator shall enter the training in ETRS.

(3) Technical Administrators. Departmental IT administrators shall ensure the control requirements applied to teleworking users of both CHP-owned and personally owned information assets are in place before connections to state

IT infrastructure are allowed. In addition, before connections are made, departmental IT administrators shall ensure the following requirements are met:

(a) Maintain Software Updates. Departmental IT administrators shall ensure information assets used to connect to the agency IT infrastructure are checked and use up-to-date operating system software and security software (e.g., antivirus, antispyware, firewall, and host intrusion prevention) every time a remote connection is initiated. This is typically accomplished through a Network Access Control solution which integrates an automatic remediation process that fixes a noncompliant information asset before allowing access to the network systems. This ensures the information asset is operating securely before interoperability with CHP IT infrastructure is allowed.

(b) Limit Telework User Privileges.

1 Each teleworking user shall have an individual user account that does not have elevated privileges. Accounts with elevated privileges create an increased security risk because they allow the user to change security settings and install applications.

2 Telework user accounts shall require two-factor authentication, except when using a web-based connection, such as Outlook Web App or other similar interfaces.

3 Telework user accounts shall, as a rule, be set up to have limited privileges. Teleworking users will not normally require accounts with full privileges (e.g., administrative accounts). In the unusual event teleworking users require administrative accounts, they shall be used only when performing authorized IT administrative tasks, such as installing updates and application software, managing user accounts, and modifying operating systems and application settings on information assets.

(c) Control the Environment.

1 Virtual private network administrators shall control the connection of client devices to the VPN concentrator with the ability to disable or disconnect active VPN sessions.

2 Split tunneling is not permitted. Only one network connection at a time is allowed. The VPN client should be configured to disallow all other connections to the computing device except for the VPN tunnel.

3 Connection to the Internet through the client computing device shall be performed through the VPN tunnel. The VPN tunnel must first be established, then a web browser may be run, and the Internet may be accessed.

4 Virtual private network gateways will be set up and managed by authorized TIS staff.

5 The latest IMD-approved version of the Cisco VPN client software will be used.

(d) Validate Control Requirements.

1 Departmental IT administrators shall log and monitor all telework access. Log files shall capture sufficient detail to allow a virtual reconstruction of the end-to-end network session. This level of detail will be necessary in the event of a breach or malware infection.

2 Departmental IT administrators shall periodically assess the controls on personally owned information assets used to connect to state IT infrastructure to ensure the information asset is operating securely before interoperability with agency IT infrastructure is allowed. This is typically accomplished automatically at each connection attempt through a Network Access Control solution which integrates an ability to deny connections made from information assets lacking the required controls.

8. ENFORCEMENT. Any employee, contractor, vendor, or agent found to have violated this policy may be subject to disciplinary action.

THIS PAGE INTENTIONALLY LEFT BLANK