CHAPTER 4

INTRANET/INTERNET

TABLE OF CONTENTS

CHAPTER 4

INTRANET/INTERNET

1. GENERAL.

   a. This chapter specifies policy and strategies for the use of Intranet/Internet technologies.

   b. Departmental computers and networks can provide access to resources throughout the world. This access requires that employees act responsibly. Employees shall respect the rights of others, respect the integrity of local and remote information systems, and observe all relevant laws and policies.

   c. All existing federal and state laws and departmental policies specific to accessing and using computer systems and exercising general personal conduct shall apply.

   d. Misuse of computing, network, or automated information resources may result in administrative action and loss of computing privileges. Moreover, misuse may be cause for prosecution under applicable state or federal statutes and/or adverse action.

2. DEFINITIONS. A glossary of terms can be found in Annex A of this chapter.

3. POLICY.

   a. Ownership of Web Pages and Files. Web pages can collate information from many different sources. As authoritative sources of information, each Office of Primary Interest (OPI) is responsible for the accuracy and timeliness of relevant Web page content. As the “owner” of specific pages and portions of pages, it is important for the responsible OPI to be part of the design and approval process of Web pages representing those subjects. The OPIs are responsible for providing complete and accurate information ready for posting. This readiness includes verifying that Web pages and related files have been completely edited and approved within the OPI. It also includes a proposed layout or description of the desired pages, although Information Management Division (IMD) is responsible for assuring the final format of the pages are in conformance with law and mandates from state organizations which have oversight responsibilities.

   b. Virus Protection. Computer users who receive or download files from remote computers shall scan the files for computer viruses before they store the files on the

network or transfer the files to others. (Refer to Chapter 5, Virus Protection, paragraph 2. of this manual.)

c. Commands will use the Internet to access remote computers where possible. The Department's direct connection to the Internet or Virtual Private Network (VPN) is a safe and reliable way to access remote computer resources.

d. In instances where necessary computer resources are not available on the Internet, commands shall contact the Help Desk to determine if connectivity can be obtained using alternative means.

e. Access to the Internet on departmentally-owned desktop or laptop computers shall be accomplished through use of the Department's network.

(1) Web browser software is installed and configured on Department-owned desktop and laptop computers; however, no Internet access method shall be used in a California Highway Patrol (CHP) facility other than network access through departmental software.

(2) Certain authorized individuals, such as designated computer forensic personnel, are exempted from this policy. All other exceptions to this policy will require the approval of the Department Information Security Officer (ISO) and Chief Information Officer (CIO), the IMD commander.

(3) Dial-up access to commercial Internet Service Providers (ISP) is expressly prohibited.

(4) Installation of Internet access software; e.g., Comcast Internet, on Department-owned computers is prohibited.

(5) Limited exceptions to the use of commercial ISPs and Internet access software may be granted by the Department ISO and CIO for departmental laptop computers used outside of the CHP network.

f. Use of Modems. In instances where neither the Internet nor a modem pool is feasible, commands may arrange to access the necessary resources using stand-alone desktop computers, modems, and standard telephone lines. Prior approval from IMD is required. Computer users shall not attach an external modem to, or install an internal modem in, a computer connected to the Department's network. To do so would subject the Department's network to access by unauthorized persons. Computer users will only attach modems to, or install modems in, stand-alone computers which do not contain confidential or sensitive information, and only with prior approval by the Department ISO and CIO.

4. INTERNET ACCESS AND USE.

a. For Business Use Only. California Highway Patrol employees may use the Internet for approved business purposes only.

b. Security and Productivity Issues. The Internet can provide a significant business benefit for state government. Effective use of Internet resources should result in more informed and productive employees. However, using the Internet raises legal, security, and productivity issues, such as the risk of downloading a computer virus, monitoring transmissions that include confidential information, and being induced by the vast social and informational forums of the Internet to spend significant work time on non-productive activities. Accordingly, the Department ISO shall routinely monitor Internet activity via proxy logs and other methods, and will make appropriate notifications to affected commanders when misuse or risky practices are detected.

c. Using the Department's Wide Area Network Computer users will access the Internet using the Department's wide area network (WAN). The network maintains firewalls and other devices that safeguard CHP resources from unwarranted intrusion.

d. Accessible Internet Sites. All departmental personnel are permitted access to an approved list of Internet sites which have been reviewed and approved through the Department's ISO. These sites may include such Internet resources as mapping sites, personnel-related sites, external law enforcement sites, weather condition sites, or other sites which are considered to be beneficial and conducive to normal business operations.

(1) Additions to Departmentally Permitted Sites. When a site is identified, which would provide useful information or services to a significant number of employees, a request with an appropriate justification may be submitted by the Division commander to the ISO requesting open access to the Web site for the Department. The ISO will make a recommendation to the IMD commander regarding access to the site.

(2) Explicitly Blocked Sites. Certain sites may be designated as prohibited for all employees. These sites may include personal electronic mail (e-mail) sites, and sites which pose legal or security risks. The ISO shall identify specific sites or categories which are to be blocked. If a user believes a site has been blocked in error or if access to a blocked site is necessary to perform assigned duties, the user shall submit a request with proper justification, through channels, to the approving Division commander. The Division commander will make recommendations regarding access to a blocked site to the Department

ISO. The ISO will make a recommendation to the IMD commander regarding removal of the site from the blocked list.

(3) Internet Access. When a user requires broader access to Internet resources than provided to all departmental employees, a CHP 109, Information Technology Request, (available in I:\Forms) shall be submitted requesting Internet access.

(4) Enhanced Internet Access. In rare instances, a small group of users may require specific access to sites which have been otherwise prohibited. Should this arise, a CHP 109 shall be submitted requesting Enhanced Internet Access.

e. Approval Authority. The final approval authority for granting Internet access privileges has been delegated to each respective Division commander. Requesters shall use the CHP 109 for obtaining command approvals. **Employees shall renew this request whenever they transfer commands.**

(1) Approved Request. Approved CHP 109 request will be signed by the employee, Area commander, Division commander, and routed to IMD, where the CHP 109 will be processed.

(2) Denied Request. Denied requests will be returned to the originating requestor by the appropriate Division, Area, or Section commander.

f. Contracting with Internet Service Providers. California Highway Patrol personnel shall not enter into contracts on behalf of the Department with an ISP for Internet access.

g. Confidential and Sensitive Information. California Highway Patrol personnel should not use the Internet to send or receive confidential or sensitive information.

h. Internet Functions.

(1) Electronic Mail. Employees may use Internet e-mail to correspond with others in the course of conducting approved business. This includes correspondence with the federal government, and any city, county, or other public agency, and with other individuals as may be necessary in the course of conducting approved business activities.

(a) To access Internet e-mail, employees must have access to the Department's Novell GroupWise or Microsoft Outlook e-mail System.

(b) Each CHP employee who has access to the Novell GroupWise or Microsoft Outlook e-mail System also has an Internet e-mail address. This address should be determined before sending e-mail messages on the

Internet so that the return address can be provided to the mail recipient. An employee's e-mail address typically is comprised of the first letter of the user's first name and the complete last name, followed by @CHP.CA.GOV. There are no spaces; e.g., Officer John Smith's e-mail address is JSMITH@CHP.CA.GOV.

(2) Other Internet Functions. Utilization of Internet functions beyond that of e-mail (e.g., Web site navigation, access to remote computer resources, and file transfer) requires prior authorization by the respective Division commander.

(a) The Department has established and will maintain a conservative approach to the use of Internet resources.

(b) To access Internet functions, other than e-mail, computer users must have access to the Department's WAN and Web browser software (e.g., Microsoft Internet Explorer). This software is normally available through the user's Netware-delivered applications.

i. Downloading or Copying Files from Internet Sources. File Transfer Protocol (FTP) allows computer users to download, or copy, files from another computer. The Internet provides access to many files stored on computers or file servers, commonly called FTP sites. A Web browser enables the user to browse FTP sites and resources. Anonymous FTP sites allow users to enter publicly accessible directories to browse and access files. Users may download files from FTP sites to their desktop computers.

j. Scanning Files for Computer Viruses. All files downloaded from the Internet shall be scanned for viruses prior to storage on the network or transfer to another employee. (Refer to Chapter 5, paragraph 2. of this manual.)

k. Monitoring Internet Use.

(1) The Uniform Resource Locator. A Uniform Resource Locator identifies the exact location or address of virtually any Internet resource. Examples include:

(a) World Wide Web Page http://www.apple.com/education

(b) Image File ftp://fabercollege.edu/graphics/flouder.gif

(c) Newsgroup news://news.lists

(d) Telnet Session telnet://ibm.com

(2) Reports to Commanders. When misuse of Internet privileges is suspected, commanders may contact the Department ISO to request analysis of individual employee Internet usage.

l. Revoking Internet Access Privileges. Division or subordinate commanders may revoke a computer user's Internet access privileges. To do so, the commander will forward an e-mail message to the Help Desk at HelpDesk@chp.ca.gov. Information Management Division personnel will verify that the message is authentic prior to taking any action.

(1) Area or section commanders who revoke an employee's Internet access privileges will send a copy of the e-mail message to the Division commander and the Department ISO.

(2) The Department ISO may identify a need to revoke a computer user's Internet access privileges. If this occurs, the Department ISO will contact the appropriate Division commander and discuss the issue.

5. WIRELESS ACCESS.

a. Scope. This section defines policy associated with wireless network access, typically referred to as 802.11a/b/g/n, Wi-Fi, or wireless local area network (LAN) access. This includes wireless access points, wireless network adapters, wireless bridges, wireless repeaters, and any other wireless networking technology utilized by the Department.

b. System Administration. The WAN Unit shall be responsible for the installation, configuration, maintenance, and other administration of all wireless LAN infrastructure hardware and software on the CHP network and/or within any CHP facility. No other parties may install, modify, or otherwise configure wireless access within any segment of the CHP network. The WAN Unit may make changes to any wireless equipment to ensure appropriate security measures are in place to minimize risks associated with wireless access.

c. Monitoring. The Security Unit, WAN Unit, and ISO may monitor any wireless network to ensure it is not being utilized in any fashion inconsistent with departmental policy. This monitoring will include, but is not limited to, authentication attempts, traffic volumes, wireless network attacks, rogue access point detection, usage patterns, and device locations.

d. Wireless Local Area Network Access. Potential users fall into several categories: (1) CHP employees with CHP equipment; (2) CHP employees with personal equipment; (3) Contractors hired by the CHP; (4) vendors or other non-CHP visitors. Wireless access may be granted as follows:

(1) California Highway Patrol Employees with California Highway Patrol Equipment. California Highway Patrol laptops may be configured to access internal network resources. Due to the high-risk nature of this access, appropriately high security levels will be applied to this access. Users requiring wireless LAN access may submit a request to the Help Desk for the configuration of their laptop.

(2) California Highway Patrol Employees with Personal Equipment. Some CHP facilities will be configured with wireless access which employees may use with their personal equipment during break times. A specific "café" network has been created which can access publicly-accessible CHP Web resources and public Internet sites. Users of this network will be blocked from certain sites which may expose the Department to legal liability, such as sites hosting malicious software or adult content. Users will be permitted to use the wireless access for other personal use, such as e-mail or personal banking. Authentication will be required to ensure that users of this network are CHP employees. Use of this "café" network is NOT permitted with CHP equipment. This network will permit only Web network protocols; i.e., HTTP and HTTPS protocols.

(3) Contractors. Contractors who will be working at the CHP for long-term engagements may have a need to use their own laptops to access non-CHP Internet resources, such as their own corporate VPN or e-mail system. These users may request CHP network accounts to permit access to internal CHP resources from CHP desktops. This account may also be used to log in using the contractor's own non-CHP equipment to the "café" wireless network similar to "CHP employees with personal equipment" above. If the contractor has a need to access internal CHP resources such as servers, file shares, or printers, they must make arrangements to use CHP equipment.

(4) Vendors and Visitors. Short-term visitors to a wireless-enabled CHP facility may request wireless access when they check in at the lobby. A set of accounts will be made available for the lobby security to distribute to vendors upon request. These accounts will remain active only for short durations, typically one business day ending at 1700 hours on the day of its issuance. These accounts will permit only Web network protocols; i.e., HTTP and HTTPS protocols. This "guest" network is not intended for use by CHP employees. California Highway Patrol employees should use option (1) or (2) above. The lobby security shall keep a record of who is granted wireless access, as well as the account name which they were issued.

e. Lobby Ambassador. California Highway Patrol Help Desk personnel will be issued lobby ambassador accounts which will permit them to create guest accounts for visitors and vendors. Typically, a set of accounts will be auto-generated for

guests. Should the quantity of auto-generated accounts be insufficient, the Help Desk can create additional accounts for use by the lobby security at wireless-enabled sites. Additional accounts should only be created at the request of the lobby security, and both the Help Desk and lobby security shall keep a record of the additional accounts which were created, who was granted access, and the account name which they were issued.

6. PERSONAL INTERNET WEB POSTINGS.

a. Scope. This section establishes policy for using official departmental logos, graphics, images, or other CHP insignias, as well as photographs, video, or any recorded images of Department peace officers, on personal Web postings, including those on social networking sites and other social media. Such sites and media include online communities and virtual sites for people who share interests and/or activities, including, but not limited to, MySpace, LiveJournal, Twitter, Facebook, LinkedIn, Flickr, etc. Employees should consider all postings on such sites as public, whether or not they have marked the site as private, locked, etc., due to the possibility of third parties importing parts of the site into the public domain. Suspects, as well as prosecution and defense attorneys, all regularly visit these sites, and CHP employees could find themselves suffering personal and professional ramifications (i.e., Brady issues) if extreme caution is not exercised.

(1) Employees have and continue to develop personal Web postings, profiles, blogs, and information on social network sites and other social media that provide information to the public about the CHP. With the exception of employees who have been trained and designated as 'Information Officers' by Office of Community Outreach and Media Relations, maintenance of a social network site and/or social media while on duty is prohibited, as well as off-duty postings that may cause discredit to the Department, and unauthorized posting of Department badges, uniforms, emblems, etc. (refer to Chapter 16 of this manual). Also, due to the possibility that, once posted, pictures, video recordings, and other images of CHP peace officers may exist in cyberspace forever, CHP peace officer employees should be aware that such postings could make them ineligible for specialized positions where anonymity is required. In addition, due to potential personal and professional ramifications of such postings, CHP employees are advised that they should obtain permission from the CHP peace officers who are in the image **prior** to posting photographs, videos, or any image of CHP peace officers on the Internet, whether or not identified as a peace officer.

Private organizations have also developed Web postings that promote their credibility or association with the CHP. Care shall be taken to ensure that

these pages do not misuse departmental insignias or otherwise misrepresent the Department.

(2) Users of CHP insignias shall do so within the best interest of the Department, cognizant of CHP's ownership rights of trademarked insignias, badges, emblems, etc., and mindful of Department policies regarding incompatible and inconsistent activities. Be advised that the Department will hold employees responsible for all postings on their Web sites or social network/media, and may take disciplinary action, up to and including dismissal, if any employee misuses CHP materials and/or images of uniformed CHP peace officers.

b. Disclaimer on Internet Web Postings. Personal Web postings, profiles, blogs, or any information on social network sites or other social media that contain Department insignias or references to the CHP, including identification as a CHP employee and/or CHP peace officer, shall include the following statement:

"THIS PAGE CONTAINS PERSONAL OBSERVATIONS AND OPINIONS OF THE AUTHOR. IT DOES NOT REFLECT THE VIEWS, NOR REPRESENT AN OFFICIAL POSITION, OF THE CALIFORNIA HIGHWAY PATROL. FURTHER, THE CALIFORNIA HIGHWAY PATROL DOES NOT ENDORSE OR APPROVE THE CONTENT OF, NOR IS IT IN ANY MANNER AFFILIATED WITH OR RESPONSIBLE FOR THE CONTENT OF THIS WEB SITE."

NOTE: This disclaimer shall be presented in uppercase and be of a font no smaller than 12 point, and shall appear on each page view.

c. Department Insignias.

(1) Outside organizations may use Department insignias only after receiving written permission from the Commissioner. Requests to use Department insignias shall be directed to IMD, who will make recommendations to the Commissioner. The final determination will be made by the Commissioner.

(2) Persons who have been determined to have misused CHP insignias shall be denied permission for future insignia use and may be subject to whatever action the CHP deems appropriate to protect CHP's ownership rights.

d. Webmaster. Issues regarding CHP-related Web pages should be referred to the CHP Webmaster in Information Technology Section (ITS). The Webmaster may be contacted by e-mail at webmaster@chp.ca.gov.

7. INTRANET ACCESS AND USE.

a. The Department's Intranet offers Web pages in the following areas:

(1) Highway Patrol Manuals.

(2) Highway Patrol Guides.

(3) General Orders.

(4) Management Memorandums.

(5) Other information about Department programs and functions.

b. Some of the documents on the Intranet are lengthy. Employees shall exercise judgment when printing these documents. It is recommended that the Publications Unit be contacted when a printed copy of a manual is required.

c. Resources Required to Access the Intranet. The user requiring access to the Intranet must use a computer which is connected to the CHP network. A Web browser is included in the standard array of software tools available on the Novell-delivered applications menu.

d. Department of Corrections Parole Law Enforcement Automated Database System. Information from the Department of Corrections Parole Law Enforcement Automated Database System is available to authorized departmental users. The Internal Affairs Section, Investigations Unit, should be contacted regarding access to this information.

8. REQUESTS TO ACCESS REMOTE COMPUTERS USING MODEMS AND STANDARD TELEPHONE LINES.

a. Commands may request approval to use modems and standard telephone lines to access remote computers when:

(1) The remote computer resources necessary are not available on the Internet.

(2) The Department's network cannot access the remote computer resources.

b. Establishing Service. The policies and procedures specified in Highway Patrol Manual (HPM) 11.1, Administrative Procedures Manual, and HPM 11.2, Materials Management Manual, shall be followed when:

(1) Establishing a contract with the provider.

(2) Paying access fees.

(3) Buying or leasing commodities.

c. Preparing the Request. A written request must be approved by the departmental ISO before access to remote computers using modems and standard telephone lines can be established or renewed. Requests shall be submitted through appropriate channels, and contain the following:

(1) Identification of the command or facility that intends to access the remote computer resources.

(2) Identification of the remote computer resources.

(3) Verification that the command has determined that the necessary resources cannot be obtained through the Department's network, or through the Internet.

(4) Identification of the business needs and benefits or opportunities associated with accessing the resources.

(5) Whether plans require establishing a contract with a provider.

(6) Identification of hardware, software, and communications commodities that must be acquired and leased, such as modems and standard telephone lines.

(7) Description of start-up and ongoing costs.

(8) Identification of the funding source for the Division.

d. Transmittal Memorandum and Certification of Compliance. A transmittal memorandum and Certification of Compliance, signed by the Division commander, shall accompany the written request.

(1) Model Certificate of Compliance. A Microsoft Word template is available on the network server. To access the model:

(a) Click on the icon for Microsoft Word, located on the applications menu.

(b) Click once on the File option.

(c) Click once on the New option.

(d) Click on the General Templates and select the template labeled MODEMS.

(e) Complete and save the document.

(2) Approved Requests. Approved requests will be signed by the Department ISO, CIO, and the appropriate Assistant Commissioner, and routed to the appropriate Division commander.

(a) The originator shall attach a copy of the approved certification to a completed Purchase Requisition in the Requisition Delivery System, and add ITS and Telecommunications Section (TS) as OPI Approvers.

(b) The originator shall simultaneously prepare a memorandum to TS, with a copy of the approved certification attached, requesting installation of the modem and model telephone line(s).

(3) Denied Requests. Denied requests will be returned to the originating Division commander by the appropriate Assistant Commissioner.

9. WEB PAGE DEVELOPMENT.

a. California Highway Patrol Internet and Intranet Web Pages. Web pages provide a means to disseminate information to the public and within the Department without the need to wait for paper reproduction and distribution. Web pages have become integral to the CHP. The material in this chapter has been developed to establish standards for Web pages and to create a review process to ensure that commands are aware of material being published on the Web on their behalf, and that the material is consistent with departmental philosophy, goals, and values.

b. Individual commands are encouraged to develop Web pages. Initial development and subsequent maintenance and revisions to Web site materials are the responsibilities of the originating command or the OPI. Information Management Division will provide advice to Web page editors, as appropriate.

c. Review/Approval Required. All Web site material must be reviewed and approved prior to being made available to the Department on the Intranet and/or to the general public on the Internet.

d. Levels of Review. All proposed pages, and pages with major changes, shall be reviewed at the next level of command to ensure that the information presented is consistent with departmental philosophy, goals, and values.

e. Compliance with State Standards. All materials for the Internet Web site must be in compliance with state accessibility guidelines.

10. WEB PAGE DEVELOPMENT STANDARDS.

a. Translations. Web pages in languages other than English must be reviewed for accuracy by Research and Planning Section. Translation services are available from one of the Department's contracted translation vendors.

b. Government Code Section 3307.5. This Section prohibits the use of a public safety officer's photograph on the departmental Internet site "if that officer reasonably believes that the disclosure may result in a threat, harassment, intimidation, or harm to that officer or his or her family."

c. Hyperlinks to Web Sites. Non-governmental sites are to be used judiciously, and the endorsement of a commercial entity must be avoided. Requests to link to commercial or non-profit sites will be approved by the Webmaster, Department ISO, and/or the Office of Community Outreach and Media Relations, as appropriate.

d. Internet Sites Available to all Employees. All employees on the CHP network have access to the Intranet, which also allows access to Internet site addresses ending in ".gov" and ".us." Hyperlinks to most sites ending with other suffixes are accessible only by employees who have been granted Internet access as detailed in Chapter 7, Access to Individual Computer/Information Systems Resources, of this manual.

e. Electronic Mail Proxies. Unless explicitly required by law, directing e-mail to specific individuals within the Department is not permitted from hyperlinks on Internet Web pages. Commands must use a proxy e-mailbox, (e.g., recruiting@chp.ca.gov), which can be obtained from the e-mail administrator. The requesting command must specify a name for the e-mail "From:" line (e.g., CHP Recruiting), and provide the names of the employees who will be allowed "proxy rights," or access, to the mailbox.

f. Processing Electronic Mail. Electronic Mail should be processed the same as any other correspondence received by the command, with the response forwarded through channels. Commands that do not wish to reply via e-mail should include a copy of the original e-mail message with their written response.

g. Electronic Mail Attachments. Employees are reminded that any attachment to an incoming e-mail message shall be screened for viruses prior to downloading it to a server. (Refer to Chapter 5 of this manual.)

h. Confidential Information. Because unencrypted data can be intercepted and read while en route, employees shall avoid the collection of confidential information through the use of e-mail messages.

i. Publications on the Intranet. Publications for electronic distribution on the Intranet shall adhere to the standards contained in HPM 1.1, Publications Management Manual, Chapter 4, Electronic Publications: Formatting and Processing, and HPM 5.1, Correspondence Manual.

j. Area/Section Command Pages.

(1) The following information must be included on individual command pages developed for the Internet Web site.

(a) Name of command.

(b) Address of command.

(c) Telephone number and/or proxy e-mail addresses for contacting the command.

(2) It is recommended that a photograph of the commander and/or a photograph of the primary office building be included on the page. Information Technology Section will maintain a library of photographs for use by developers. A list of available photographs may be obtained from the Webmaster.

(3) Additional Web pages including information specific to a command or business unit shall be approved by the requesting Division.

11. WEB PAGE DEVELOPMENT FUNCTIONAL ROLES.

a. Information Management Division.

(1) Information Management Division is the technology branch of the CHP, and is responsible for the provision of accurate and timely electronic information to the CHP community and its related users.

(2) While individual commands are responsible for the development of information to be posted on the Internet and Intranet servers, IMD is responsible for the coordination of all Web-related projects and owns all Web pages which do not contain material that is clearly the responsibility of another OPI.

b. Information Technology Section.

(1) Information Technology Section is responsible for assuring that all mission critical computer systems, including the Internet and Intranet servers, are available 24 hours per day, seven days per week.

(2) Information Technology Section is also responsible for maintaining backup copies of all data. Standard production and change controls will be applied by ITS to ensure the integrity and reliability of data.

(3) The Infrastructure Services Group (ISG) of ITS is responsible for posting approved material to the Department's Web sites.

(a) Pages will be initially posted to a test area on the server. The developer will be notified of the location at which the new pages can be viewed.

(b) The developer shall review their pages in the test environment and submit any final necessary changes to ISG.

(c) Once testing is complete and the pages have been deemed to meet the needs of the developing command, ISG staff will schedule the posting of the pages and notify the command when the pages have been made available in the production environment.

c. Web Editor.

(1) Overview. As authoritative sources of information, each OPI is responsible for the accuracy and timeliness of relevant Web page content.

(2) Objectives. Web pages provide a means to disseminate information to the public without the need to wait for paper reproduction and distribution. Web pages have become integral to the CHP. Policy has been developed to establish standards for Web pages and to create a review process to ensure commands are aware of material being published on the Web on their behalf, and the material is consistent with departmental philosophy, goals, and values. Individual commands are encouraged to develop Web pages. Initial development and subsequent maintenance and revisions to the Web site materials are the responsibilities of the originating command or the OPI. Information Management Division will provide advice to Web page editors, as appropriate.

(3) Expectations of Divisions. In order to maximize the usefulness of Web pages, Divisions which have Web content will work with IMD to ensure the accessibility and accuracy of the information being presented. Divisions are expected to appoint a Web editor and an alternate Web editor, and appoint

staff to fill subsequent vacancies. Every effort will be made by IMD to minimize the demands on these employees relating to Web pages.

(4) Expectations of Web Editors. Web editors shall gather and prepare content for Web pages (whether unique to the OPI or required by Top Management); review it for accuracy; and obtain approval of requesting Division to proceed with a new page creation.

(a) If a new or revised official publication (Management Memoranda, HPM, etc.) will reside in the Department's online Publications Library, interaction should occur with the OPI for the library, Assistant Commissioner, Staff, Publications Unit.

(b) Please allow IMD extra lead time for:

1 The preparation of images, illustrations, online movies, or complex tables not already in a digital format;

2 The creation of proxy e-mail boxes;

3 Or features not approved by existing procedure or Executive Management, yet still considered to be of vital importance.

(c) Submit to IMD for review:

1 Accessibility and branding issues.

2 Copyright infringement prevention.

3 Navigation aids.

4 Initial testing of hyperlink validity.

5 Dependency on technologies that may not be universally installed or available (e.g., browser plug-ins or separate "helper" applications not in widespread use).

6 Privacy concerns, including the collection and use of information from visitors.

7 The absence of proprietary (browser-specific) characteristics. Web pages should be viewable by a wide array of Web browsers running on any operating system.

8 Schedule for posting.

(d) Review Web documents (generally when posted in "test" or "staging" regions). Explicit written direction is required to indicate Web pages are in their "final" form and are ready for public viewing.

(e) Periodic review of posted Web pages (and hyperlinks) for accuracy and currency should be performed at least every 180 days. Web editors and their Divisions are responsible for the accuracy of information appearing on the Web pages. Information Management Division should not be expected to monitor the accuracy of information.

d. Webmaster.

(1) Role. The primary role of the Webmaster is to act as liaison between CHP Web technology and the user community within the Department. The Webmaster shall foster Web page development throughout the Department which conforms to the standards found in this chapter.

(2) Responsibilities.

(a) Policy and Review. The Webmaster develops policy concerning Web site usability and the maintenance of Web materials, and administers all review processes for the accuracy, function, and quality of Web pages on CHP sites. The Webmaster does not review the content or relevance of material submitted for inclusion on departmental Web sites.

(b) Site Planning. The Webmaster shall review proposed Web pages to determine how they interface with current pages and other proposed pages, to verify the absence of copyrighted material for which written approval has not been obtained, and to confirm their compliance with state accessibility guidelines. The Webmaster shall be available to meet with page developers to discuss options and guidance for the presentation of information, and will make the determination of which CHP site (Internet or Intranet) is the most appropriate location for the material to reside.

(c) Coordination with the Academy's Graphic Services Unit. The Webmaster shall work with the Academy's Graphic Services Unit (GSU) to develop graphics that present the CHP in a professional manner. The Webmaster, in conjunction with ISG, will establish a library of graphic images and photographs that may be used by all page developers.

(d) Electronic Mail Response. The Webmaster is designated as the first-line respondent to e-mail inquiries from the Internet and Intranet. These messages will typically arrive at the GroupWise mailboxes "webmaster" and "webadmin", to which the Webmaster has proxy rights. Some CHP commands have developed Web pages with their own proxy mailboxes

(e.g., CHP Recruiting). Response to an e-mail sent to a specific command via proxy shall be handled by the command or OPI for the relevant Web pages.

e. Web Oversight Committee. The Web Oversight Committee (WOC) is an IMD standing committee formed to assist IMD in the creation of policy concerning new technology, compliance issues, and overall Web site design. Committee members and their roles are as follows:

(1) Information Management Division Chief. The IMD chief is the chair of the WOC.

(2) Information Security Officer. The Department ISO will ensure the Department's information security policies, especially those applicable to Web pages, are followed. The Department ISO will review proposed pages for hyperlinks to pages outside of the CHP environment to ensure those pages do not present a security risk to the Department or the users. Pages shall also be reviewed for accuracy and organizational sensitivity.

(3) Graphic Services Unit. The GSU will review pages for artistic appeal, common look and feel, and general presentation of material. The GSU will assist in developing graphics and providing images or photographs for use by departmental developers.

(4) Office of Community Outreach and Media Relations. The Office of Community Outreach and Media Relations will review pages for organizational sensitivity and concurrence with current departmental philosophy, and will ensure that proposed pages do not present information conflicting with any other departmental page or publication.

(5) Headquarters and Field Command Representatives. Representatives from headquarters commands will review pages for consistency, presentation, uniformity with other pages and publications of the command, and to ensure compliance with publications standards.

(6) Infrastructure Services Group Representatives. Representatives of ISG will review pages for adherence to standards, ensure that the graphics or photographs used on a particular page are available on the Web server, and verify that the proposed page(s) can be accommodated on the server. After all approvals are received, ISG staff will post the proposed pages to the test area of the Web server for review by the developer. Once the developer has determined that the pages are accurate and display correctly, ISG staff will post them for general availability.

12. WEB PAGE DEVELOPMENT PROCEDURES.

a. Assistance. Page developers are encouraged to meet with the Webmaster and ISG staff for design assistance prior to the commencement of page development.

b. New and Updated Material.

(1) Command Level. Pages shall first be reviewed and approved at the command level. The commander's review is critical in ensuring that pages accurately reflect the command's work, properly represent the Department, and are sensitive to the needs of the user(s). A proposed Web page should be reviewed as critically as any other document being forwarded for review within the chain of command.

(2) Chain of Command Review. Proposed Web pages and major Web page revisions shall be reviewed by the next level of command prior to submission to the Webmaster.

(a) Submissions - New Material. After review and approval by the requesting command, the normal process for adding material to a CHP Web site is:

1 Complete a CHP 53, Request for Information Technology (IT) Services, which can be found in I:\Forms.

a In the "Detailed Description of Request" field, include:

1/ The intended audience for the new material.

2/ Any coordination that will be required with other initiatives, campaigns, or media types (such as video).

3/ The OPI which will monitor the material for accuracy and currency.

4/ Present and future requirements for providing the material in languages other than English.

5/ The suggested date of implementation or availability.

6/ For information that is of a temporary nature, the "sunset" date after which the material can be removed.

7/ The name of a contact person who can provide additional clarification upon request.

b In the “Business Justification” field, state the reasons or the potential benefits for adding the material.

2 Submit the completed CHP 53 to IMD accompanied by:

a Physical or digital files containing the text and images which are to be made available. Prototypes, approximate page layouts, and samples can also be included. Digital copies of images for the Web pages should be forwarded with the CHP 53. This will ensure quicker posting of content to the Web.

b Electronic source documents, such as Microsoft Word files, must be submitted whenever possible.

3 Requests that are incomplete or incorrectly formatted will be returned.

4 Upon approval by all levels of command, the appropriate Assistant Commissioner will have the final review authority for the content or appearance of Web pages.

(b) Minor Updates. Minor updates usually do not require the addition of a Web page, and may be submitted directly to the Webmaster. Approval of the requesting command is to be obtained before minor updates are made. Examples of minor changes include, but are not limited to:

1 Substitution of a photograph or graphic image.

2 Correction of a typographic error.

3 Change in area code or telephone number.

4 Replacement of the name of a unit or commander.

5 Update of information in a statistical table.

(c) Webmaster Review. The Webmaster is the last step in the normal review process for proposed Web material and updates. Compliance with policy governing the use of copyrighted material, effective Web site structure and navigation, and the presentation of information to those with disabilities will be confirmed.

(3) Posting of Pages.

(a) Test Pages. Once all appropriate approvals are received, pages will be posted in a test area on the Internet or Intranet Web server. The Webmaster will notify the developer via e-mail that the pages are available for review.

(b) Approved Pages. If the developer is satisfied the pages display correctly, they should notify the Webmaster via e-mail, and the pages will be moved to the production environment.

(c) Disapproved Pages. If the developer does not approve of the pages, they must make the desired modifications and re-send the pages to the Webmaster, for reinstallation and additional review by the developer.

This review shall also include a confirmation that hyperlinks remain active, and pages continue to display correctly. The developer shall make any necessary changes to the pages, have them approved through the chain of command (as necessary), and resubmit them to the Webmaster for reposting.

(b) Conformance with Policy. A concurrent periodic review shall also be conducted by the Webmaster, who will notify the developer if matters of concern arise.

THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX A

DEFINITIONS

1. DEFINITIONS.

a. Internet. The Internet is a worldwide network of computer networks, connected by data links. It is used for a variety of functions such as e-mail, remote access to computer data banks, and file transfer. The Internet operates under decentralized control, as opposed to the operation of on-line services that are controlled by the person or organization that provides the service.

b. Intranet. The Intranet is a more limited collection of computer networks that is not intended to be accessed by the general public. It is a private network and cannot be accessed by persons outside the organization, except as authorized by the organization, and is protected by "firewall" software.

c. Web Site. A Web site is a specific address for files which can be accessed from the World Wide Web. Each site has a home page, which is the first document the user of a Web browser sees when they enter the site.

(1) The address (or URL) for the Department's Internet site is www.chp.ca.gov.

(2) The URL for the CHP Intranet site is home.chp.ca.gov.

d. Browser. A Web browser is a software application used to locate and view information on both the Internet and Intranet. Microsoft Internet Explorer and Netscape Communicator are the departmental standard Web browsers.

e. Hyperlink. A hyperlink is an image or highlighted text in a Web document which, when selected, will load information from another Web document (or a different location in the same document) into the Web browser.

f. Plug-In. A plug-in is a hardware or software module that adds a specific feature or service to the user's browser. Plug-ins are frequently used to play audio or video files, view animated presentations, and may also be used to view different forms of text.

2. STANDARDS FOR WEB PAGE PRESENTATION.

a. Universal Access. Web pages must be constructed in such a manner that they can be viewed with any popular Web browser software.

(1) Any of the Microsoft Office Suite of applications (for Intranet page development).

(2) Microsoft Notepad.

(3) Microsoft WordPad.

(4) Generic text editor applications (on systems which do not use operating system software from Microsoft).

(5) RealNetworks Helix Universal Server.

(6) Apple Streaming Video Server.

(7) Macromedia HomeSite.

(8) Any of the Adobe Systems' design, publishing, video, or Web tools.

(9) Adobe Acrobat (if generated by the software products listed above, and enhanced with accessibility "tags," and accompanied by either an equivalent HTML page or a link to equivalent text on another Web page – for Internet page development).

c. General Page Design Considerations.

(1) Developers shall design Web pages for viewing on computer monitors set to display at 800 pixels by 600 pixels resolution, unless the information being presented illustrates a compelling motivation for assuming a different aspect ratio.

NOTE: The actual dimensions of the area that is displayed within a fully opened Windows-compatible browser are 780 pixels (width) by 460 pixels (length).

(2) Internet Web pages that are most likely to be printed by visitors may be accompanied by an equivalent "printer friendly" version of the page.

(3) Whenever possible, the preeminent information should already be visible in the browser window when the Web page loads. If scrolling down repeatedly will be required to see the entire contents, consider dividing the content into multiple Web pages.

(4) Spelling and punctuation must be verified.

d. Images, Photographs, and Graphics.

(1) Guidelines for Internet Web pages specify that "the use of graphics should be at a minimum," and should be used only "to help in a description or to understand what is being said" on a Web page.

(2) All images (other than background images) must include an HTML 'ALT' parameter. This is to provide information to Web page visitors who are unable to see the image. For non-decorative images, 'ALT' text should serve as a self-contained replacement for the unique content of the image, and usually not as a mere description of it.

(3) Any information conveyed only by an image must be accompanied by a text equivalent, such as the image's HTML 'ALT' parameter, an equivalent HTML page or a link to equivalent text on another Web page.

(4) Information conveyed by the use of color must be accompanied by an equivalent HTML page or a link to equivalent text on another Web page.

(5) Image maps, table cells, and other colored or delineated page regions cannot be used on Internet Web pages to connote meaning or content unless there is an HTML or text equivalent on the same Web page (or linked from that page).

(6) Formal photographs (head shots), when viewed in a Web browser, shall not exceed a size of 150 pixels in width by 200 pixels in height.

e. Formatting Text for Hyperlinks.

(1) Hyperlinks specified in CHP pages must refer to currently active sites/pages. It is the responsibility of the command/OPI developing the page to periodically review all hyperlinks on their pages to ensure that they are linking to active pages. Inactive hyperlinks must either be updated or removed.

(2) Hyperlinks to non-governmental sites are to be used judiciously, and the endorsement of a commercial entity shall be avoided. Requests to link to commercial or non-profit sites will be closely reviewed by chain of command and final approval will be granted by the ISO.

(3) Hyperlinks to government or law enforcement sites are permitted. Some governmental entities use Web site addresses that do not have a ".gov" suffix; care should be taken to request that the ISO approve the addition of these sites to the list of those universally accessible by all CHP employees.

(4) Specifying colors for hyperlinked text is to be avoided on Intranet sites, and is not permitted under the mandated guidelines for Internet Web pages.

(5) All employees on the CHP network have access to the Intranet, which also allows access to sites with URLs ending in ".gov" and ".us." Hyperlinks to most sites ending with other suffixes are accessible only by employees who have been granted Internet access. (Refer to Chapter 7 of this manual.)

f. Electronic Mail Hyperlinks.

(1) Commands who wish the user to be able to contact them by e-mail may use a "mailto:" hyperlink on their Web pages, which will invoke the visitor's e-mail client software.

(2) The use of additional parameters (e.g., "mail to:webmaster@chp.ca.gov?Subject=home page") is not permitted, due to extremely unreliable processing of such by the client software.

g. Scripts and Programs. Scripts and programs that execute on the "client" PC can make information unobtainable by Web site visitors using assistive technology and shall not be used on Internet Web pages without a waiver from IMD. The use of scripts and programs on Intranet Web pages must be approved in advance by the Webmaster and/or the ISO, after full consideration of the operational ramifications. Such functions include:

(1) Programs.

(2) Scripts.

(4) Authentication, controlled access, or encryption technology.

(5) Audio or music.

(6) Video or animation.

h. Plug-Ins.

(1) Developers shall not construct pages that require the user to obtain a plug-in in order for the page to display. The only exception is the Adobe Acrobat text reader plug-in. This plug-in is free to all users and will not result in departmental liability.

(2) Plug-ins cannot be used on Web pages without the prior approval of IMD after full consideration of the operational ramifications.

i. Pages Under Construction.

(1) "Under Construction" text or icons are generally used to denote that a page or site has been proposed but is not yet ready for viewing.

(2) Unless previously approved by IMD, "Under Construction" pages shall not be displayed on CHP Web sites.

j. Indicators of New Web Pages or Content.

(1) "New" icons or text may be used on newly posted pages. The "new" designation should be removed not later than 30 days after the page has been posted.

(2) It is the responsibility of the page developer to remove (or request the removal of) the graphic or text representation of "new" from the page.

k. Copyrighted Material. Copyrighted material shall not be used unless permission has been granted, in writing, from the copyright holder.

l. Templates.

(1) Mandated guidelines for Internet Web pages specify the template (the stylistic “framework”) that shall appear on all Internet Web pages.

(2) Standardized templates shall be used on all Intranet Web pages. Pages not conforming to the templates must be approved in advance by IMD. To obtain the templates, contact the Webmaster by sending an e-mail to GroupWise recipient name “CHP WebAdmin@chp.ca.gov.”