CHAPTER 1

GENERAL

TABLE OF CONTENTS

ANNEXES

CHAPTER 1

GENERAL

1. PURPOSE.

a. Information Assets. The state's information assets are an essential public resource. The unauthorized destruction, tampering, modification, deletion, or disclosure of information included in agency files and databases can compromise the integrity of state programs, violate individual rights to privacy, and constitute a criminal act. Accordingly, the Department must assume responsibility for the proper classification, use, and protection of its automated information. Additionally, the Department has established risk management and disaster recovery planning processes for identifying, assessing, and responding to the risks associated with its information assets.

b. Protection Guidelines. California Highway Patrol (CHP) employees and other authorized computer users are responsible for protecting the Department's information technology assets. Highway Patrol Manual (HPM) 40.4, Information Security and Administration Manual, has been developed to provide guidance for the use and protection of these assets.

2. POLICIES AND PROCEDURES.

a. The CHP is responsible for ensuring its information technology assets are protected from damage, destruction, and unauthorized or accidental modification, deletion, access, or disclosure.

b. Pursuant to the requirements of State Administrative Manual (SAM), Chapter 5300, et al., internal policies and procedures are necessary in the following areas:

(1) Assignment of management responsibilities for information technology risk management.

(2) Appointment of a Department Information Security Officer (ISO).

(3) Provision for the integrity and security of automated information produced or used in the course of agency operations.

(4) Provision for the security of information technology facilities, software, and equipment utilized for automated information processing.

(5) Establishment and maintenance of an information technology risk management program.

(6) Maintenance of a risk analysis process.

(7) Compliance with the state audit requirements relating to the integrity of information assets.

(8) Compliance with state reporting requirements.

3. INFORMATION SECURITY OFFICER.

a. The ISO oversees agency compliance with policies and procedures regarding the security of information and information processing assets. The ISO reports to the Department's Chief Information Officer and executes the responsibilities of the office in an effective and independent manner. The agency director has ultimate responsibility for information technology security and risk management within the agency. The ISO is not responsible for information processing, technology operations, or for agency programs that employ confidential information.

b. The ISO manages the Department's information security program. The information security program has five important objectives:

(1) Protect the Department's information and information processing assets.

(2) Manage vulnerabilities within the information processing infrastructure.

(3) Manage threats and incidents affecting the agency's information resources.

(4) Ensure, through policy, the appropriate use of the Department's information resources.

(5) Ensure employees are aware of their responsibility to protect and secure information.

c. The Department ISO's top priority is security and risk management. Responsibilities include:

(1) Implementing procedures to ensure the establishment and maintenance of a security and risk analysis program.

(2) Establishing security policies and procedures designed to protect information assets, including the necessary controls required to prevent

unauthorized access to systems and data files, program documentation, and equipment.

(3) Identifying vulnerabilities that may cause inappropriate or accidental access, destruction, modification, or disclosure of information, and establishing the security controls necessary to eliminate or minimize potential impact.

(4) Establishing of procedures necessary to monitor and ensure compliance with established security and risk management policies and procedures.

(5) Coordinating with commanders that have experienced any loss of personal information as defined in Civil Code Section 1798.29 and complying with the applicable notification requirements.

(6) Ensuring the Department is in compliance with the security reporting requirements pursuant to Information Technology Policy Letter 10-13, Security Reporting Scorecards.

(7) Submitting incident reports to the California Technology Agency (CTA), Office of Information Security (OIS), as required by the SAM and the State Information Management Manual (SIMM).

(8) Collaborating with fiscal auditors to define their role in automated information systems planning, development, implementation, operations, and modifications to security and risk management.

(9) Collaborating with Information Management Division (IMD) on matters related to planning, developing, implementing, or modifying information security and risk management policies and procedures that affect the Department.

(10) Testing of the Department's Disaster Recovery Plan (DRP).

(11) Acquiring security equipment and software.

(12) Ensuring all CHP employees have completed the required security awareness training on an annual basis.

(a) Responsible for providing the security awareness training. The ISO will also audit and evaluate the process to ensure adherence to the Department's information privacy program.

(b) The ISO is responsible for updating the security awareness training.

(c) The ISO must certify and submit on an annual basis to the CTA that privacy guidelines have been developed, that training and education programs exist and are conducted on an annual basis, and that internal control evaluations are in place to ensure compliance with the agency's information privacy program.

4. CLASSIFICATION OF DATA.

a. Confidential and Sensitive Information. State Administrative Manual, Chapter 5320.5 (refer to Annex A of this chapter) identifies two classes of information that require extra precautions: Confidential Information and Sensitive Information.

(1) "Confidential Information - information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws." An example of confidential information would be personnel documents, personnel rosters including personal information, or investigative materials. The key factor for confidential information is its dissemination.

(2) "Sensitive Information - information maintained by state agencies that requires special precautions to protect from unauthorized modification or deletion."

(a) Sensitive information may either be public or confidential, and requires a higher than normal assurance of accuracy and completeness.

(b) An example of sensitive information would be records of departmental financial transactions. The key factor for sensitive information is its integrity.

(3) The owner, author, or originator of the data will determine its classification.

(4) Data addressed to a specific person may also be classified *personal and confidential*.

b. Privacy Information (Civil Code Section 1798.29). Privacy information is defined as first name or first initial and last name in combination with social security and/or driver license number, and/or an account number, credit or debit card number in combination with any required security code, access code, or password. Privacy information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

c. Employee Responsibilities. Computer users will ensure that all confidential and privacy information are reasonably secure and not open to scrutiny.

(1) Employees shall not leave computers accessing/displaying confidential information unattended.

(2) Confidential information shall not be stored on a computer that is not password protected or subject to controlled access. Passwords shall be changed on a scheduled basis. Passwords used by prior employees of a command are to be deleted.

(3) Employees shall obtain departmental approvals prior to using personally-owned computers or electronic devices (i.e., USB/flash drives, portable hard drives, smart phones, tablets) for work-related activities. Requesters shall use the CHP 109, Information Technology Request, for obtaining command, Division, appropriate Assistant Commissioner, ISO, and IMD approvals. Employees shall renew this request whenever they transfer commands. Employees shall insure that all data containing confidential or privacy information is encrypted and password protected.

NOTE: Refer to HPM 11.2, Materials Management Manual, Chapter 18, Privately Owned Laptop Computer and Word Processor Repair/Replacement Policy, for additional guidelines.

(4) Compact Discs, Digital Video Discs, flash drives, removable discs, and other forms of computer information storage media containing confidential files and privacy information shall be securely stored.

(a) Confidential information may be provided only to those designated to receive it.

(b) Reports specifying instances or attempted instances of inappropriate data access shall be reviewed by the Department ISO and the appropriate Division chief.

(c) Magnetic tape or other appropriate electronic storage media shall be used to store backup copies of the Department's valuable information at an approved off-site location.

(5) Personnel and Command Rosters. All confidential and/or sensitive departmental work products maintained by a command shall be assessed to determine the need for continued storage.

(a) All confidential and/or sensitive departmental work products and rosters maintained by a command and needed to conduct state business shall be secured **at all times**.

(b) All confidential and/or sensitive departmental work products and rosters maintained by a command and needed to conduct state business shall be placed in a locked cabinet/container after normal business hours.

(c) Only authorized departmental employees shall have access to confidential and/or sensitive departmental work products.

(6) All employees, volunteers, and contractors are required to complete security awareness training on an annual basis. The training will include a section that describes consequences of violating departmental information privacy policies.

d. Commander's Responsibility.

(1) Maintain an inventory of the electronic data systems and storage media in use within their commands that contain privacy information subject to Civil Code Section 1798.29. The inventory should indicate if the data is encrypted or not.

(2) Establish and maintain local controls, to be included into Area Standard Operating Procedures, outlining local notification procedures to be taken in the event of a potential breach of data.

(3) Commanders shall ensure only authorized departmental employees have access to confidential and/or sensitive information, as well as departmental equipment.

(4) Commanders shall ensure only designated personnel having an after-hours need for the rosters have access to the secured/locked cabinet/container.

(5) Commanders shall ensure all employees under their command have completed the required security awareness training on an annual basis. The Security Awareness and Privacy Training is located on the CHP Intranet. The training can be taken manually by printing out the document and completing the test or can be completed online.

(a) Employees shall review the material and complete the test. Once completed, the employee shall certify the training by signing the privacy acknowledgement form. Acknowledgement forms shall be retained in the employee's personnel file.

(b) The command's training coordinator shall enter the training in the Employee Training Records System.

(c) Commanders shall submit a memorandum, certifying employees who completed the training and listing those who have not fulfilled the requirement. The list of those who have not completed the training shall include the employee's name, reason training was not completed, and the anticipated date the training will be completed. The memorandum shall be forwarded through channels to their respective Division, who in turn shall consolidate the reports and submit through channels to IMD. Commands shall develop a plan to ensure those individuals who missed the training are provided training upon the employees' return to work.

(d) The ISO will compile Division reports into one consolidated departmental report.

(e) The Department ISO will notify the CTA through channels.

e. Destruction of Confidential and Sensitive Information.

(1) Authorized users shall always take care to properly dispose of computer-generated sensitive and confidential data. This includes the destruction of printouts or records which contain social security numbers, names and identification numbers, addresses, home telephone numbers, etc.

(2) Confidential and sensitive information shall be destroyed by cross-shredding, by placing the information in a confidential destruct container, or by appropriately obliterating the confidential information in a manner that will ensure that it is unattainable by others.

(3) All computer hard drives, including those from workstations, laptops, mobile digital computers, and file servers leaving departmental control for purposes of repair, replacement, or to be surveyed, shall be electronically scrubbed (all data overwritten) prior to release, in a manner approved by the Department ISO.

(4) Owners of data/records shall identify a retention schedule of all records within a database for disposal purposes.

(5) Outdated rosters or those no longer needed by the command shall be destroyed by cross-shredding and handled as confidential and/or sensitive information, before being discarded.

5. FACSIMILE AND SCANNED DOCUMENTS SECURITY.

a. Facsimile (fax) machines and computer systems with fax capability are not normally to be used to send or receive confidential or sensitive information.

b. When there are no other alternatives available, employees may transmit sensitive and confidential information using fax machines, and computer systems with fax capabilities, only when the information is transmitted from one secure location to another secure location.

c. Employees should take necessary steps to verify that the information arrived securely; e.g., a follow-up telephone call.

d. The use of autodial capabilities is highly encouraged when routinely faxing this type of information to a specific location.

e. It is permissible to fax California Law Enforcement Telecommunications System (CLETS) information from one secure location to another secure location. Both the CHP command and person faxing the information and the person/agency receiving the information are responsible for its security. Employees are reminded that all CLETS information is confidential and for official use only by authorized law enforcement or criminal justice personnel.

f. Scanned documents containing confidential, sensitive or personnel information shall be encrypted before sending the document to another party via electronic means (i.e., electronic mail [e-mail], file share, file transport protocol). If the document is to be stored electronically it must be kept in a secure folder location which only authorized individuals have access to.

6. COMPUTER SECURITY GUIDELINES.

a. The Department's information systems are a vast configuration of resources, many of which contain sensitive and confidential data. It is the responsibility of every user to protect these assets and take a proactive role in preserving CHP data and associated computer resources/equipment. Accordingly, the Department will follow generally accepted industry standards to secure its information systems.

b. Computer Room Access. Employees shall not allow unauthorized personnel to enter computer rooms, server facilities, or telephone closets. Only employees with a legitimate need shall have access to computer rooms and server facilities or telephone closets. Commanders of these facilities are responsible for updating access lists regularly.

c. Networking Component Access. Employees shall not allow unauthorized personnel access to networking components. Networking components include file servers, hubs, routers, telephone lines, message switching systems, computer

aided dispatch (CAD) interfaces, and similar types of networking or computer equipment.

d. Personal Computer Access. Employees shall not allow unauthorized individuals to use their desktop or laptop computers for any reason.

(1) Computer users shall not leave desktop computers accessing/displaying confidential information unattended. Desktop computers are not to be left logged on when the user is away from their desk. Users may lock the computer (example: Ctrl, Alt, Delete, and Enter) if temporarily away from the computer.

(2) Laptop computers shall be in a secure place when not in use, and are not to be left unattended when in use.

e. Equipment.

(1) Commands shall use standard equipment, as determined by IMD.

(2) All computer hardware shall be tagged with a CHP identification tag.

(3) Data circuits shall be supplied by IMD, who will have control and/or oversight of all system design, cabling, data circuits, and installation.

(4) Whenever possible, commanders shall make provisions for CHP equipment such as servers, hubs, and routers to be in locked cabinets or in rooms with controlled access and shall make provisions to control access to phone closets which contain the command's network connection.

(5) Department labels and/or specifically colored jacks should be used to identify CHP computer-related equipment.

(6) These provisions are applicable to equipment purchased by or donated or gifted to the Department.

(7) The connection of any personally-owned desktop/laptop computer or device(s) (e.g., printers, scanners, plotters, USB flash drives, wireless access points, removable hard drives, network switch/hubs) to the Department's network is strictly prohibited. The consequences of an inadvertent infection of our systems can be severe. To ensure compliance with departmental information technology security requirements and to minimize the risk of system exposure, only standard desktop/laptop computers and/or devices approved for purchase by IMD, and identified with a valid CHP-numbered decal, can be connected to the network.

(a) Information Management Division recognizes that there will be an occasional need for exception to this policy. In those instances where the computing need cannot be met, approval may be granted, after consultation with IMD, once the following questions have been affirmatively/satisfactorily answered:

1 Business justification for connection to the Department's network.

2 Identification of encryption software brand and version utilized on the personal desktop/laptop computer.

3 Identification of virus protection software brand and version utilized on the personal desktop/laptop computer.

4 Identification of the method used to update virus patterns.

(b) Requesters shall use the CHP 109 for obtaining command, Division, ISO, and IMD approvals. Employees shall renew this request whenever they transfer from commands.

(c) Approved Request. The approved CHP 109 request will be routed through channels to IMD for processing. The CHP 109 shall be returned to the employee's field folder and a copy will be filed with the Information Technology Section (ITS).

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

7. INFORMATION OWNERSHIP.

a. Commands that are the designated owners of information, automated files, or databases will be responsible for the following:

(1) Classifying each file or database in accordance with the need to control access and preserve the security and integrity of the file or database (refer to Annex A of this chapter).

(2) Taking precautions for controlling access to, and preserving the security and integrity of, the files and databases that require such measures.

(3) Authorizing access to information in accordance with the classification of information and need to access.

(4) Monitoring to ensure compliance with the information security policies and procedures of the CHP and the State of California.

b. Performance of these responsibilities is required throughout the life cycle of the file or database. Owners of automated files and databases shall coordinate these responsibilities with the Department ISO.

8. INFORMATION CUSTODIANS.

a. The custodian of an automated file or database shall comply with:

(1) Applicable law and administrative policy.

(2) Any additional security policies and procedures established by the owner of the automated information and the Department ISO.

(3) Identified retention schedules of all records located within a database for disposal purposes.

b. The custodian shall advise the owner of the information and the Department ISO of vulnerabilities that may present a threat to the information and of specific means of protecting that information.

c. The custodian shall notify the owner of the information and the Department ISO of any actual or attempted violation of security policies, practices, and procedures.

9. RISK ANALYSIS TEAM.

a. The CHP has established a multidisciplinary Risk Analysis Team as required by SAM, Chapter 5305.1. The Department ISO is the chair of the team.

b. The Risk Analysis Team includes representatives from IMD, Administrative Services Division, and Emergency Operations and Safety Services Section. The team meets once every quarter to assess the vulnerability of information technology assets and to develop contingency plans. The team's analyses and recommendations are presented to Executive Management. Vulnerabilities to be assessed include:

(1) Accidental acts such as errors, omissions, modifications, destruction, disclosure, negligence, and interruption of utilities.

(2) Intentional acts such as theft, fraud, embezzlement, misuse, misappropriation, extortion, forgery, unauthorized disclosure, and physical or logical sabotage, such as computer viruses.

(3) Natural catastrophes such as fires, floods, and earthquakes.

10. DISASTER RECOVERY PLAN.

a. Requirements. State Administrative Manual, Chapter 5355.2, (refer to Annex B of this chapter) requires the Department to maintain a DRP. The plan shall identify critical computer applications, information assets that are necessary to support those applications, and plans for resuming business operations following a disaster that affects critical applications. The Department will test the DRP periodically.

(1) State Administrative Manual, Chapter 5355.2, stipulates the following filing requirements:

(a) Submitting an informational copy of the DRP to the CTA by April 15 of each year.

(b) Because the Department contracts with the CTA, Office of Technology Services (OTech) for services, a copy of the DRP shall be forwarded to that agency.

(2) If there are no changes to the previous year's plan, the Commissioner may submit a certification to that effect rather than resubmit the plan.

b. Responsibility. The Department Disaster Recovery Coordinator is responsible for the oversight of the disaster recovery program. The preparing, testing, and maintaining of the DRP is a combined effort of all sections under IMD.

c. Content. The DRP shall cover a minimum of ten subject areas as listed in SIMM Section 65A, Disaster Recovery Documentation for Agencies Preparation Instructions:

(1) Agency Administrative Information.

(2) Critical Business Functions/Applications.

(3) Recovery Strategy.

(4) Backup and Offsite Storage Procedures.

(5) Disaster Recovery Procedures.

(6) Data Center Services.

(7) Resource Requirements.

(8) Assignment of Responsibility.

(9) Contact Information.

(10) Testing.

d. Disaster Recovery Coordinator.

(1) The Department's ISO has been designated as the Department's Disaster Recovery Coordinator.

(2) The Department's Disaster Recovery Coordinator shall have sufficient knowledge of information management and information technology to work effectively with the OTech and the vendors necessary to re-establish information processing and telecommunications services after the occurrence of a disaster.

e. Disaster Recovery.

(1) Information Management Division will direct ITS, Infrastructure Services Group (ISG), to recover or repair the existing system.

(2) Information Technology Section, ISG, will also be directed to initiate concurrent work to identify and establish the system at another site(s).

(a) Select Network Administrators, Network Coordinators, and technical support staff will attempt to recover existing file servers, and repair equipment such as hard disks, memory, and other circuitry, and restore software, documents, and files.

(b) Select Network Administrators, Network Coordinators, and technical support staff will also identify another site(s), and initiate procedures to establish the system at that site(s).

11. DOCUMENTING DAMAGE OR DESTRUCTION OF STATE ASSETS.

a. Incidents involving intentional damage or destruction of state assets will be documented in writing.

b. Commanders will promptly investigate incidents involving intentional damage or destruction of state assets when the estimated value of the assets exceeds $2,500.

c. Commanders will also investigate incidents of unauthorized or accidental modification, destruction, disclosure, loss, or access to automated files and databases, and incidents involving loss, damage, or misuse of information technology assets.

d. The commander shall forward a copy of the report to the Department ISO through the appropriate Division chief.

e. The Department ISO will complete an Information Security Incident Report for forwarding to OIS.

12. MISUSE OF INFORMATION.

a. The California Legislature has found that the protection of the state's computers, computer systems, and computer data is vital to the protection of the privacy of individuals. It is also necessary for the well-being of financial institutions, business concerns, governmental agencies, and others within this state who lawfully utilize those computers, computer systems, and data. Penal Code Section 502 establishes penalties for unauthorized access to computers, computer systems, and computer data. (Refer to Chapter 6, California Law Enforcement Telecommunications System, paragraph 2.k. of this manual.)

b. Any employee who misuses automated information is subject to disciplinary action. The Department will take appropriate action, which may include dismissal and the submission of criminal evidence to the local district attorney.

c. Violations may also result in civil action being taken against the employee, the employee's supervisor, and/or the Department.

d. Any misuse of information which has been accessed through CLETS, or any violation of law or CLETS rules, regulations, or operating procedures, may result in action taken by the Department of Justice (DOJ) against the CHP. Sanctions may include a letter of censure, suspension, or termination of CLETS service.

e. The downloading, installation, configuration, and/or operation of game software or game demos on CHP-owned computers is expressly prohibited. If authorized software includes game components, the person authorized to load such software must remove or disable any included games if it is possible to do so.

f. Storing or transmitting files (including data or programs) not used for departmental purposes, such as music, programs, picture images, previews, and "movie" images using CHP-owned equipment or CHP networks is prohibited.

13. SANCTIONED INVESTIGATIONS.

a. During the course of a criminal or administrative investigation, individual commands may conduct investigative searches of local area network e-mail, files, documents, printed records, or CLETS transactions. These searches are only

authorized for criminal or administrative investigations, and shall have the prior approval of an appropriate departmental manager and the Department ISO. The investigating command shall notify the Department ISO, who will make the necessary arrangements for the specific accounts to be searched. Requests for such records may be submitted by either memorandum or e-mail to the Department ISO. The request must come from the appropriate departmental manager.

b. Only the Office of Internal Affairs (OIA), with the approval of the Department ISO, has the authority to approve the ongoing monitoring of a specific account.

(1) Monitoring an e-mail account is defined as the ability to view or retrieve copies of e-mail messages as they occur or shortly after each transmission or reception.

(2) Commands desiring to monitor e-mail messages on a continuous basis shall request permission from the OIA and Department ISO.

c. The Department ISO shall be notified when an internal investigation is being conducted which involves accessing information the Department maintains by way of electronic or paper means.

(1) The Department monitors all Management Information System (MIS) transactions which can be identified by terminal mnemonic, user identification, date, and time.

(2) The DOJ monitors all CLETS transactions and has the ability to flag individual files to identify inquiries. Requests for assistance with possible breaches of CLETS security shall be made to the Department ISO, not DOJ.

d. All identified instances of unauthorized disclosure, access, loss, or misuse of data shall be reported to the Department ISO.

14. PROGRAM DEVELOPMENT.

a. New or planned information technology projects will be evaluated by the Department ISO for security risks.

b. Information Management Division will include the Department ISO in discussions of new applications and program development work. This will enable the Department ISO to address security issues during the beginning stages of an information technology project.

c. Information Management Division will forward a copy of all Feasibility Study, Special Project, and Post Implementation Evaluation Reports to the Department ISO, who will determine if the Risk Analysis Team needs to assess the information.

15. MANAGEMENT INFORMATION SYSTEM USE BY NONPERMANENT EMPLOYEES.

a. The MIS may be used by temporarily hired persons such as youth aids, annuitants, or senior volunteers.

b. Each individual shall successfully meet the background requirements outlined in Chapter 6, paragraph 2.h. of this manual.

c. Each individual shall complete and sign a CHP 101, Appropriate Use of Automated Information & Systems Statement, (available in I:\Forms).

d. Each individual shall successfully meet the training requirements outlined in Chapter 6, paragraph 5. of this manual.

16. MANAGEMENT INFORMATION SYSTEM USE BY ALLIED AGENCIES.

a. The use of MIS by an allied law or non-law enforcement agency or representative may be authorized by the Department ISO.

b. A memorandum shall be sent, through channels, requesting approval by the Department ISO.

c. Allied agency personnel shall sign a CHP 101.

d. Each individual requesting access to MIS shall successfully meet the background requirements outlined in Chapter 6, paragraph 2.h. of this manual. If the individual has not been previously fingerprinted by their agency, the requesting CHP command will arrange for fingerprinting.

e. A user identification shall be assigned to each individual.

f. A statement of understanding shall be prepared and placed in the command file for each allied agency representative requesting the use of MIS. The memorandum will be tailored to meet the needs of individual commands. If a command has chosen to allow unlimited use of equipment by a particular agency; e.g., the Department of Motor Vehicles, one Memorandum of Understanding (MOU) per year will suffice. Areas requiring assistance with the content of the MOU should contact Business Services Section, Contract Services Unit. The MOU should contain:

(1) Dates equipment is to be used.

(2) Name of allied agency involved.

(3) Signatures of persons in charge of the allied agency.

g. Non-law enforcement agencies shall be required to pay for all equipment and line costs associated with access to MIS.

h. Non-law enforcement agencies shall not have access to CLETS.

17. REMOTE ACCESS TO CALIFORNIA HIGHWAY PATROL AUTOMATED SYSTEMS AND INFORMATION BY OUTSIDE ENTITIES.

a. Outside entities, e.g., non-law enforcement governmental agencies, media, value-added resellers, automobile clubs, private companies or organizations, or other individuals not employed by the CHP, may apply for access to departmental automated systems/information on a restricted basis.

(1) Remote access is defined as:

(a) Dialing-in to a CHP system via modem to a specified port on the system (e.g., access to the CHP CAD system via the media port).

(b) Dialing-in to an intermediary source, such as the Freeway Incident Response System Tracking (FIRST), via modem to view CHP information.

(c) Remote support of CHP computer system(s) by non-CHP employees through either secure dial-in connection or secure Internet connection.

(2) Two-way communication is defined as the dynamic free flowing exchange of information between a CHP system and the user of the system.

(3) While “read only” access may be granted, there shall be no two-way communication between outside entities and CHP systems.

b. Access to information resources will be coordinated with IMD and the Department ISO to ensure adherence to CHP and DOJ policies.

(1) Applications shall be approved by the Department ISO.

(2) Requests shall be submitted through appropriate channels.

(3) Requests shall include the purpose and justification for access.

c. The following requirements and restrictions will be placed on any entity requesting access to departmental information resources:

(1) Confidential or sensitive information such as investigative reports, personnel, medical, and other automated records, personal names, social security numbers, telephone and cellular telephone numbers, pager numbers, home addresses, CHP identification numbers, driver license and/or registration information, witness, suspect, or victim personal information contained in departmental information systems shall not be divulged to outside entities, except as permitted by law.

(2) The Department's networks shall not be used by outside entities as a means of communication with departmental employees.

(a) Outside entity users shall not be given e-mail accounts on the CHP e-mail network in order to communicate with CHP employees.

(b) Outside entities may use Internet e-mail to communicate with designated employees or positions.

(c) Requests for exception to this prohibition may be made to the Department ISO, who will examine the circumstances of the request before making a determination.

(3) Once approval is received from the Department ISO, outside entities may access information systems such as FIRST via telephone lines.

(a) System design shall include a form of authentication protection, such as a physical token device and password or other industry security standard.

(b) System design shall be approved by the Department ISO.

(4) A program agreement shall be signed by the business, corporation, allied agency, or organization prior to access approval being granted.

(a) The CHP will provide the format for the program agreement.

(b) The agreement shall define the roles, obligations, and conditions associated with each participant.

(c) The agreement shall be approved and signed by the Department ISO and the executive officer of the requesting organization.

(5) Entities requesting access to CHP information systems shall read and sign a CHP 101A, Agreement With Outside Entities to Establish Remote Access Privileges to CHP Automated Computer Systems and Information, (available in I:\Forms).

(a) This agreement will ensure that users are notified and are aware of the policies, laws, and penalties for the misuse of computer-generated information.

(b) The CHP 101A shall be renewed every year and kept on file locally for the term of the agreement or until a new form has been signed. A copy of the signed CHP 101A shall be forwarded to the requesting entity.

18. PROHIBITION OF TWO-WAY COMMUNICATION/UPDATE CAPABILITY WITH CALIFORNIA HIGHWAY PATROL COMPUTER AIDED DISPATCH SYSTEMS.

a. Two-Way Communication. Two-way communication (the dynamic free flowing exchange of information between a CHP system and the user of the system) is normally prohibited with CHP CAD systems. Requests for exception to this prohibition may be made to the Department ISO, who will examine the circumstances of the request before making a determination.

b. Update Capability. Update capability means the ability to directly modify an entry in a record or log, or the ability to add additional information to an existing record or log.

c. Departmental Users.

(1) A limited number of CHP information systems permit two-way communication and update capability by departmental employees.

(2) Employees shall have received training on the use of these systems and their security constraints, and in some instances shall have passed proficiency tests, prior to being granted update capabilities. Supervisory oversight of employees with update capabilities shall be maintained wherever possible.

(3) Update capability for the CHP CAD systems shall be restricted to trained and authorized communications and/or Transportation Management Center personnel.

(4) Manual updates by other than communications or Transportation Management Center personnel shall be routed through a CAD position(s) designated by the Department ISO. The designated individual(s) will determine if an update is necessary and initiate appropriate update action.

Requests for designation shall be submitted by memorandum through channels.

d. Non-Departmental Users.

(1) Two-way communication with CHP CAD systems shall not be permitted for non-departmental users outside of communications or Transportation Management Centers.

(2) Requests for exception to this prohibition may be made to the Department ISO, who will examine the circumstances of the request before making a determination.

(3) The CAD systems shall not be updated by non-departmental users outside of communications or Transportation Management Centers.

ANNEX A

STATE ADMINISTRATIVE MANUAL, CHAPTER 5320.5

SAM - Chapter 5300

5320.5 CLASSIFICATION OF INFORMATION
(Revised 10/09)

Subject to executive management review, the agency unit that is the designated owner of a record (paper or electronic, including automated files, or databases) is responsible for making the determination as to whether that record, file, or database should be classified as public or confidential. and whether it contains personal and/or sensitive data. The owner of the record, file, or data is responsible for defining special security precautions that must be followed to ensure the integrity, security, and appropriate level of confidentiality of the information.

The state's records, automated files, and databases are essential public resources that must be given appropriate protection from unauthorized use, access disclosure, modification, loss or deletion. Each agency must classify each record, file, and database using the following classification structure:

1. Public Information – information maintained by state agencies that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

2. Confidential Information – information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

Sensitive Information and Personal Information, as defined below, may occur in Public Information and/or Confidential Information. Records, files, and databases containing sensitive and/or personal information require special precautions to prevent inappropriate disclosure. When confidential, sensitive, or personal information is contained in public records, procedures must be used to protect it from inappropriate disclosure. Such procedures include the removal, redaction, or otherwise masking of the confidential, sensitive, or personal portions of the information before a public record is released or disclosed.

While the need for the agency to protect data from inappropriate disclosure is important, so is the need for the agency to take necessary action to preserve the integrity of the

data. Agencies must develop and implement procedures for access, handling, and maintenance of personal and sensitive information.

1. Sensitive Information – information maintained by state agencies that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher-than-normal assurance of accuracy and completeness. Thus, the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency financial transactions and regulatory actions.

2. Personal Information – information that identifies or describes an individual as defined in, but not limited by, the statues listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request.

a. Notice-triggering personal information – specific items or personal information (name plus Social Security Number, driver's license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. See Civil Code Sections 1798.29 and 1798.3.

b. Protected Health Information – individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. State laws require special precautions to protect from unauthorized use, access, or disclosure. See Confidentiality of Medical Information Act, Civil Code Sections 56 et seq. and the Patients' Access to Health Records Act, Health and Safety Code Sections 123100-123149.5.

c. Electronic Health Information – individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers that conduct electronic transactions to ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure. See Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164.

d. Personal Information for Research Purposes – personal information requested by researchers specifically for research purposes. Releases may only be made to the University of California or other non-profit educational institutions and in accordance with the provisions set forth in the law, including the prior review and approval by the Committee for the

Protection of Human Subjects (CPHS) of the California Health and Human Services Agency before such information is released. See Civil Code Section 1798.24(t).

THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX B

STATE ADMINISTRATIVE MANUAL, CHAPTER 5355.2

SAM - Chapter 5300

5355.2 AGENCY DISASTER RECOVERY PLAN

(Revised 10/09)

Each state agency (including each state data center) must maintain a Disaster Recovery Plan (DRP) identifying the computer applications that are critical to agency operations, the information assets that are necessary for those applications, and the agency's plan for resuming operations following an unplanned disruption of those applications.

Each agency that employs the services of a state date center must develop an understanding of the existing service level agreement for recovery services, and its recovery plan must document the data center services that will be required during recovery.

Each agency must keep its DRP up to date and provide annual documentation for those updates to the Office. The annual requirements are:

1. Each agency must file a copy of its DRP and the Agency Disaster Recovery Plan Transmittal Letter (SIMM Section 70D) with the Office, in accordance with the Agency Disaster Recovery Plan Submission Schedule.

2. If the agency employs the services of a state data center, it must also provide the date center with either a full copy or a subset of its plan, containing enough information for the data center to recover the agency's systems and/or data.

3. AN Agency Disaster Recovery Plan Certification (SIMM Section 70B) may be filed in place of a full DRP if both of the following conditions exist:

    a. A full plan was submitted the previous year and is on file with the Office.

    b. No changes are needed to the current plan.

4. Each agency DRP must cover, at a minimum, ten topic areas which are listed and describe directed in SIMM Section 65A. If the agency has not developed a full business continuity plan, three supplemental DRP requirements must be included as directed in SIMM Section 65A. In addition, if the DRP does not follow the format in

SIMM Section 65A, a cross-reference sheet (see SIMM 70D) must be included with the update to indicate where information on each topic can be found in the DRP.

It is important to adapt the detailed content of each plan section to suit the needs of the individual agency, with the understanding that DRPs are based upon available information so they can be adjusted to changing circumstances.