INFORMATION SECURITY OFFICE

Information Security Policies

August 2010

Table of Contents

100 Purpose 4
110 Scope & Applicability 4
120 Authority & Policy Maintenance 4
130 Disclosures 4
140 Roles & Responsibilities 4
150 Information/Data Policy 8
160 Information Classification 8
170 Information Security Principles 9
180 Regulation & Enforcement 10
190 Variance Process 10
200 Access Controls 10
210 Access Management 10
220 System Access Controls 11
230 Remote Access & Teleworking 12
240 Remote Control 13
250 Wireless Computing 13
300 Awareness & Training 14
310 Information Privacy & Security Awareness Training 14
400 Audit & Accountability 15
410 Monitoring System Access 15
420 Audit Logs 16
430 Log File Retention 16
440 Audits 17
500 Certifications & Security Assessments 17
510 Vulnerability Assessment Scans 17
600 Configuration Management 17
610 Configuration & Change Management 17
620 Unnecessary System Services 18
700 Disaster Recovery Planning 18
710 Disaster Recovery Management 19
720 System/Data Back-ups 19
730 Off-site Storage 19
800 Identification & Authentication 19
810 Authentication 19
820 Password Authentication 19
900 Incident Reporting & Notification 20
910 Incident Reporting Roles & Responsibilities 21
920 Information Security Violations to be Reported 22
1000 Maintenance 23
1010 System Maintenance Policy & Procedures 23
1020 Controlled Maintenance 23
1100 Media Protection 23
1110 Media Transport (Mobile Computing & Removable Storage) 23
1120 Media Allocation 24

1130 Media Physical Security 24
1140 Media Tracking & Recovery 25
1150 Media Maintenance 25
1160 Media Sanitization & Disposal 25
1200 Physical & Environmental Protection 26
1210 Physical Security 26
1220 Environmental & Security Controls 26
1300 Planning 27
1310 System Security Plan 27
1400 Personnel Security 27
1410 Security & Confidentiality Acknowledgements 27
1420 Access Agreements 28
1430 Separation and Transfers 28
1500 Risk Assessment 28
1510 Risk Management 28
1520 Risk Analysis 28
1600 System & Services Acquisition 30
1610 Software Licensing, Copyrights & Intellectual Property 30
1620 Technical Documentation 30
1700 System & Communications Protection 30
1710 Firewalls 30
1720 Telecommunications & Network Security 31
1730 Encryption 31
1740 Communications Methods/Data Transmission 32
1800 Security & System Integrity 32
1810 Patch & Vulnerability Management 32
1820 Server Configuration & Hardening 33
1830 Hardware/Software Upgrades 33
1840 Application Development 33
1850 System Testing & Training 34
1860 Virus Protection 34
1870 Workstation Security 34
1880 Malicious Mobile Code 35
1890 Intrusion Detection & Prevention 36
1900 Acceptable Use of Information Technology Resources 37
1910 E-mail Messages & Instant Messages 38
1920 External E-mail & Instant Messaging 39
1930 File Sharing 39
Appendix A: Forms Index 40
Appendix B: Glossary 41
Appendix C: Information & Data Handling 43
Appendix D: CDPH Social Networking Guideline 46
Appendix E: Sample CDPH Warning Banner 48

100 Purpose

The Department is required to ensure the security, privacy, integrity, availability, accountability, and the means to audit its information. This policy provides a general framework that shall be followed when handling Department information and using Department resources.

110 Scope & Applicability

This policy applies to information, resources, and employees as defined below.

- The term "information" is defined as oral, paper or electronic records, files, databases and any other means of storing data.
- The term "resources" is defined as information technology (IT) facilities, software, and equipment owned or leased by State agencies. This includes mobile devices such as a Personal Computer (PC), Personal Digital Assistant (PDA), Smartphone (i.e. Blackberry device), Compact Disk (CD), Laptop, cellular phone, Tablet PC, (Universal Serial Bus) USB drive, and other similar devices.
- The term "employee" includes all Department employees, contractors and student assistants working in Department facilities who have access to Department information.

Additional terms used within this Policy are defined in Appendix B, Glossary.

120 Authority & Policy Maintenance

The Chief Information Security Officer (CISO) is responsible for maintaining this Policy. Final review and approval of policy content is the responsibility of the Director or the Director's designee.

Any comments, questions, corrections, or changes to this Policy are to be submitted to the CISO.

130 Disclosures

Employees are granted access to Department information to perform their job functions on a need to know basis. Employees shall have no expectation of privacy from Department monitoring and inspection in the use of Department resources. The Department reserves the right to monitor, log and/or inspect all activity in the use of these resources. All Department IT equipment is subject to inspection and possible forensic analysis by the IT Division or Internal Audits at any time.

140 Roles & Responsibilities

Security is everyone's responsibility and everyone has a role in protecting CDPH information resources.

Director

The Director has ultimate responsibility for information security, privacy, risk management, and disaster recovery planning at CDPH. On an annual basis, the Director shall certify that CDPH is in compliance with State policy governing information security, risk management, and privacy programs. (See SAM Sections 5305, 5315, and 5360)

Chief Information Officer (CIO)

The CIO has overall responsibility for all aspects of the Department's information resources and IT systems, and directs the use of IT to support the Department's goals.

Chief Information Security Officer (CISO)

The CISO has overall responsibility for ensuring the confidentiality, integrity, and availability of information resources within the Department. The CISO oversees compliance with information security laws, policies, standards, and procedures.

CISO's responsibilities include:

1. Promoting awareness of information security issues among management and staff.
2. Ensuring sound security principles are reflected throughout the organization's vision and goals.
3. Evaluating and communicating security related information.
4. Establishing and maintaining security policies and procedures.
5. Monitoring and certifying compliance to policies and standards.
6. Reporting to external control agencies.

Privacy Officer

The CDPH Privacy Officer is responsible for the privacy of all information/data maintained by the Department and the legally permissible users and disclosures of confidential, sensitive, or personal information.

Privacy Officer's responsibilities include:

1. Ensuring the maintenance of the Department's Privacy Program Policies when the Department collects, uses, maintains, discloses, or disposes of personal or confidential information.
2. Minimizing the impact on individual's and organization's privacy, particularly an individual's personal information dignity, while achieving the vital public health objectives and duties required of the Department.
3. Obtaining complete reports from Programs on such incidents and overseeing and approving corrective action plans.
4. Overseeing and ensuring the Department's implementation of and compliance with State and Federal privacy laws, including the California Information Practices Act (IPA) and the Federal Health Insurance Portability and Accounting Act (HIPAA) privacy regulations.

Managers & Supervisors

All CDPH Managers and Supervisors must:

1. Ensure their staff receives information privacy and security awareness training and education. (See Section 310, Information Privacy & Security Awareness Training)
2. Ensure that all employees understand the confidential nature of information under their control and the procedures for maintaining privacy, confidentially and security. Also ensure that all employees understand applicable Federal, State and Department policies concerning information, equipment, privacy and security, and possible penalties for illegal and unauthorized use or release of confidential information. Monitor and enforce compliance of staff to these policies. (See Section 150, Information/Data Policy)
3. Based on *principle of least privilege*, approve the appropriate level of access to information resources only to staff whose business function has been authorized for access by the Information Owner. (See Section 210, Access Management)
4. Ensure processes are in place to immediately remove information resource access of staff when they separate from CDPH to change business functions and no longer have a business need for access. (See Section 1430, Separation & Transfers)
5. Annually review and ensure appropriate information system access is given to staff. (See Section 210, Access Management, and Section 220, System Access Controls)
6. Ensure that sufficient resources and appropriate staff are available to establish and maintain Internet activities in a responsible manner. Ensure all content placed on the Internet, regardless of source information, is approved in accordance with existing information release policies and procedures prior to placement on the Internet and/or E-mail.
7. Define and document security requirements and project specifications prior to initiate Internet or E-mail projects and submit them to the IT Division for approval.
8. Ensure that no contracts with, or procurement of, commercial or private Internet Service Providers (ISPs) for either Internet or E-mail activities are made without prior approval from the CIO and the CISO.
9. Ensure that web site content is accurate, relevant, and current including references to non-Department resources, such as other State or Federal agencies.
10. Ensure that no classified data is released by the Department to external entities in violation of Federal or State laws or regulations, or Department policies; and that non-routine releases of such data in large quantities are approved by the CISO and the Privacy Officer in writing before being made.

Information Custodians

Information Custodians are made up of Local Area Network (LAN) Administrators, Information Technology (IT) Administrators and other IT staff.

All Information Custodians must:

1. Comply with applicable laws, administrative policies and security policies and procedures established by the Information Owners and CDPH Executive Management. (See Section 200, Access Controls)
2. Advise the Information Owner and the CISO of vulnerabilities that may present a threat to the information and of specific means of protecting that information.
3. Ensure that the necessary technical means are in place to preserve the confidentiality, integrity, and availability of the Department's information resources and manage the risks associated with those resources.
4. Ensure that individuals other than Department employees are not granted access to the Department network or any State computer systems, without obtaining prior approval from

both the Division Chief overseeing those individuals and the ISO. (Use CDPH 9058, Foreign Computer Attach Request; See Appendix A)
5. Support the use of existing Department infrastructure, technologies, policies, procedures, standards and guidelines in using, developing, or making information available on the Internet.
6. Route all application, Internet or E-mail related Interagency Service Requests through the IT Division and ISO for approval.
7. Ensure that the following are not established without obtaining prior approval from the CIO and ISO: local area networks or modem connections, including point-to-point or serial line IP connections or virtual private networks (VPNs), on existing local or wide area networks, Internet/web servers, proxy servers, firewalls, or client browsers configured to access a proxy server.
8. Ensure that measures are taken to prevent malicious or otherwise destructive or damaging software (e.g., computer viruses, worms, Trojan horses or other malware) from destroying or causing damage to files and operating systems. Therefore, all servers and workstations connected to the Department network, and/or that store or transmit Department information, shall be a part of the Department's centrally managed anti-virus program.

Information Users

Information Users are any staff that use CDPH information and/or resources. This includes CDPH employees, contractors, retired annuitants and student assistants.

All Information Users must:

1. Use Department information and resources only for CDPH business purposes in accordance with their job duties. (See Section 1870, Workstation Security, and Section 1900, Acceptable Use of IT Resources)
2. Complete mandatory annual Information Privacy and Security Awareness Training regarding the Department's information security policies, and sign acknowledgements of their information security responsibilities, Security & Confidentiality Acknowledgement (CDPH 2420 Form). (See Section 310, Information Privacy & Security Awareness Training, Section 1410, Security & Confidentiality Acknowledgements, and Appendix A, Form Index)
3. Comply with applicable laws, administrative policies, and security policies and procedures established by the Information Owner and CDPH Executive Management. (See Section 150, Information/Data Policy, Section 1900, Acceptable Use of IT Resources, and Appendix D, CDPH Social Networking Guideline)
4. Notify the Information Owner and the CISO of any actual or attempted violations of security policies, practices or procedures. (See Section 900, Incident Reporting & Notification)

Information Owner

Information Owners are any staff that collect and maintain information on behalf of CDPH. Guidance for Information Owners can be found in SAM 5320.1.

All Information Owners must:

1. Classify the information resources within their areas of program responsibility. (See Section 150, Information/Data Policy, and Section 160, Information Classification)
2. Define precautions to protect and preserve the confidentiality, integrity, and availability of the information resources.

3. Based on the *principle of least privilege*, authorize the appropriate level of access to the information resources only to business functions having a business need to access the information. (See Section 220, System Access Controls)
4. Ensure program staff and other users of the information are informed of, and carry out their information security responsibilities.

150 Information/Data Policy

State and Federal law, as well as Department policy, require privacy and security protection of all confidential, sensitive and personal information, in whatever medium (oral, paper or electronic), handled by the Department. The definitions of public, confidential, sensitive and personal information are set forth in Section 160, Information Classification.

The Department considers all information about individuals private unless such information is determined to be a public record. It is Department policy to maintain records and equipment privacy measures that protect privacy and prevent the loss of information through accident, misuse, sabotage or other criminal activity, or natural disaster.

The California Information Practices Act (IPA) is the legal authority for State agency privacy safeguard policies, along with the Health Insurance Portability and Accountability Act (HIPAA), which is more recent and applies only to records in the possession of Department health plans or providers covered by HIPAA, such as Emergency Medical Services Appropriation (EMSA), Pre-Natal & Infant Screening Program, AIDS Drug Assistance Program (ADAP), Viral & Rickettsial Disease Laboratory (VRDL), etc.

Electronic files and databases shall be given appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion. Files and databases should be protected according to the classifications. (See Section 160, Information Classification, and Appendix C, Information & Data Handling) Access to confidential, sensitive, and personal data in the Intranet and/or Extranet must use the principles of least privilege and need to know.

160 Information Classification

For purposes of information security and privacy protection, Department information is classified as follows:

1. Public Information - information maintained by the Department 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. (See SAM Section 5320.5)

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. (See SAM Section 5320.5)

3. Sensitive Information - Information maintained by the Department 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 Department's financial transactions and regulatory actions. (See SAM Section 5320.5)

4. Personal Information - Information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. (See SAM Section 5320.5)

    a. Notice-Triggering Personal Information - Specific items of personal information (name plus Social Security Number (SSN), 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 Sections1798.29 and 1798.3)

    b. Protected Health Information (PHI) - 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 Section 56 et seq., the Patients' Access to Health Records Act, Health and Safety Code Section Sections 123100-123149.5, and the HIPAA Privacy Rule at 45 C.F.R. 164.514)

    c. Electronic Protected Health Information (ePHI) - 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 HIPAA, 45 C.F.R. 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))

Releases of confidential, sensitive, or personal data to external entities, which are not required by Federal or State laws or regulations or Department program policies, shall be approved by the CISO and the Privacy Officer (in writing) before transmission.

170 Information Security Principles

The Department must design, implement, and manage all information systems as such:

- Apply the *principle of defense in depth* to provide the appropriate physical and logical layers of security.
- Apply the *principle of least privilege* to access controls of all information resources.
- Apply the *principle of separation of duties* to reduce the risk of collusion.
- Apply the *principle of need to know*, access to information must be necessary to complete one's duties.
- Monitor all information systems for unauthorized intrusions and system misuse/abuse.
- Comply with CDPH policies and all applicable State and Federal laws and regulations.
- Provide standards, procedures and guidelines in support of Policy.

- Authorize, authenticate and uniquely identify all users of information resources.
- Periodically and independently review the effectiveness of security controls applied to information systems.
- Provide Information Security awareness and education to users of CDPH information resources.
- Ensure that all information systems are designed to ensure the confidentiality, integrity and availability of our information assets.

180 Regulation & Enforcement

The Director, or the Director's designee, is responsible for ensuring compliance with provisions of this Policy and the administration of the following duties, which include, but are not limited to:

1. Investigating alleged or suspected non-compliance within the provisions of this Policy.

2. Suspending service or employee access to resources when deemed necessary for the operation and/or integrity of the State communications infrastructure or connected networks.

3. Proceeding in accordance with Department progressive discipline and civil service rules because of non-compliance with this Policy.

4. Monitoring and/or logging all network activity.

190 Variance Process

A variance is the temporary authority to continue or implement a solution when Information Security Policy compliance cannot be achieved. The variance request must include a plan for compliance and be submitted to the ISO for consideration. Use a CDPH Form 9069 to submit a request for variance.

If approved, a variance will be granted for a maximum of one (1) year. Upon expiration, the issue is reevaluated to determine if compliance has been achieved. If not, the ISO may grant or deny an extension. If denied, the issue may be escalated to a higher authority.

200 Access Controls

210 Access Management

As it relates to access management, SAM Section 5320.2 states that Information Owners are responsible for:

1. Authorizing access to the information resources for which they have ownership responsibility in accordance with the classification of the information and the need for access to the information. (See Section 160, Information Classification)
2. Defining precautions for controlling access to and preserving the security and integrity of files and data bases that have been classified as requiring such precautions. (See Appendix C, Information and Data Handling)

CDPH Information Owners authorize access to the information resources for which they have ownership responsibility by:

1. Identifying and documenting the business functions with a business need for access to the information.
2. Identifying and documenting the minimum level of access needed by those functions to perform their job duties based on the classification of the information and the *principle of least privilege.*

CDPH Managers and Supervisors must review requests for physical and system access to information resources and approve only those for individuals who:

- Have signed a CDPH confidentiality agreement form. (See Appendix A, Forms Index: Security & Confidentiality Acknowledgement, CDPH 2420 Form)
- Have passed the personnel screening process.
- Have completed the Information Privacy and Security Awareness Training.
- Perform a business function that has been authorized for access by the Information Owner.

CDPH Managers and Supervisors must apply the *principle of least privilege* to ensure that only the access that is needed is approved.

CDPH Managers and Supervisors must revoke access to information resources immediately for staff that separate from CDPH or no longer perform the authorized business function. (See Exit Clearance, CDPH 2005 Form)

Information Custodians are responsible for documenting, implementing and maintaining the access management controls required by the Information Owner and Federal, State and CDPH regulations, policy and standards.

At a minimum, the following access controls must be established:

1. An annual review process designed to update the accuracy of access granted to information resources.
2. A process to ensure information is secure when users access confidential data from a remote location by the use of notebooks, laptops, mobile phones and other remote access methods.
3. A process to review, suspend and/or delete access if the user has not accessed the data within a specified time, based on the system owners requirements, but at a minimum on an annual basis.
4. A process to ensure that an employee's access to confidential data is suspended when or if they fail to complete annual Information Privacy and Security Awareness Training within a reasonable time.
5. A process to address suspected or known reportable unauthorized access in accordance with established Department policy. (See Section 900, Incident Reporting and Notification)

220 System Access Controls

Information Owners and Information Custodians of all CDPH systems, with the review and approval of the CDPH ISO, must restrict those functions and processes that can be misused to compromise

the security or availability of systems and information. These functions and processes may include, but are not be limited to, any applications, system functions, utilities, transactions, or information that can be misused to compromise the confidentiality, integrity, or availability of CDPH information or systems, or to disable security protections.

Effective system access controls must be established and maintained to:

1. Present an approved warning banner each time a user attempts access to any CDPH computer system, regarding the confidentiality of the data in the system and the consequences for unauthorized access and use. The user must acknowledge and accept the terms and conditions of the banner prior to system access. The acceptance of the acknowledgement must be logged. (See Appendix E, Sample CDPH Warning Banner)
2. Restrict access to confidential information to individuals authorized by the Information Owner. Access to such information must be provided upon the specific identification and authentication of the individual.
3. Control access to restricted functions. All such access must be provided upon the specific, individual identification and authentication of the person or entity.
4. Immediately disable authorization to perform functions or obtain information upon notification of compromise.
5. Automatically disable accounts used for authentication after three unsuccessful logon attempts. Access may be manually or systematically restored after a predetermined time period.
6. Configure workstations, servers and other personal computing devices to automatically lock system access if unused for fifteen (15) minutes. Users must have the capability to manually lock the system without logging off.

Users must be granted rights and privileges only on a "need to know" or only on a need-to-use basis and according to the *principles of least privileges*. When system users have elevated privileges (such as LAN, IT and Database Administrators), they must consider the access control requirements contained herein as minimum standards. Where possible, these Administrators must employ more stringent access control measures.

230 Remote Access & Teleworking

Security requirements shall be followed at remote locations, although they may be implemented in different ways. For example, paper-based confidential, sensitive, or personal information must be locked up when not in active use. When traveling, confidential, sensitive, or personal information must not be separated from the employee if possible. In no case shall such information be left unattended in vehicles or checked with baggage on a commercial airplane. (See Removal of Classified Information, Section 1820)

1. **Inbound Connections to Department Networks:** All inbound connections and connection methods to Department internal networks and/or multi-user computer systems shall be ISO approved remote access solutions.

2. **Authentication:** Remote access to Department computers and networks will require that all users use two-factor authentication. Users shall be authenticated by identification systems approved by the ISO. All users working remotely shall connect to Department computers and internal networks via authorized communications methods.

3. **Discarding Confidential Information When Off-Site:** Employees shall not discard confidential information in home or hotel wastebaskets, publicly accessible trash containers,

or store such information in public storage lockers. Instead, this information shall be retained by the employee in locked rooms, files, cabinets or other containers until it can be destroyed by shredding, or other approved methods, at Department facilities or other approved locations. (See Safeguards for Handling Classified Information, Section 1810)

Teleworking uses communications technology to enable staff to work remotely from a fixed location outside of their organization. Suitable protection of the telework site must be in place against vulnerabilities such as theft of equipment and information, unauthorized disclosure of information, unauthorized remote access to the organization's internal systems, or misuse of facilities. It is important that teleworking is both authorized and controlled by management, and that suitable arrangements are in place for this method of working. CDPH will only authorize telework activities if appropriate security arrangements and controls are in place according to CDPH's Telework Program Policy and Procedures. The following physical security concepts should be considered at the telework site:

- Take into account the physical security of the building and the local environment;
- The proposed telework environment;
- The communications security requirements, the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and pass over the communication link, and the sensitivity of the internal system;
- The threat of unauthorized access to information or resources.

This policy applies to all users authorized to remotely connect to the Department's network and applies to any computing device that authorized users may use.

240 Remote Control

Due to possible dangers associated with enabling remote control software (e.g., VNC, PCAnywhere, GoToMyPC, LapLink, and many more), CDPH shall only permit its use upon completion of a formal risk analysis and written approval by the ISO. The ISO's approval shall be consistent with the Department's software and architectural standards.

250 Wireless Computing

When remotely accessing the Department's network, the use of wireless technology is subject to the same controls and requirements as other methods of remote access. The authorized remote user must be trained on the proper use of wireless technology, and the wireless device must be configured according to established CDPH security standards.

Risks go up when wireless networking capabilities are directly connected to a secure wired network. Without proper controls, wireless communications may penetrate (or circumvent) CDPH's defenses and provide a compromised back channel. Wireless is unguided and broadcast signals can travel several hundred meters. This policy is concerned with electronic devices that contain wireless telecommunications capabilities and are, or could be, connected to the CDPH sensitive data stores. Wireless technologies include, but are not limited to:

- Wireless local-area networks (WLAN)/wireless metropolitan-area networks (WMAN);
- Wireless peer-to-peer connections (includes the entire electromagnetic spectrum);
- Wireless E-mail devices (e.g. Blackberry devices, Personal Digital Assistants (PDAs), smart phones (web-based enhanced cell phones connected to the Department's network), etc.);

- Laptops or notebook computers;
- Data input terminals (i.e., bar code scanners for inventory control);
- Wireless desktop workstations (i.e. personal computers);
- Two-way pagers that interface with CDPH's enterprise network;
- Wireless keyboards and other input devices.

This policy targets wireless capabilities that have the potential to connect to the Department's secure enterprise network. All wireless technology hardware and software must conform to the current CDPH standard. CDPH will use approved encryption at all times during wireless transmissions. CDPH's wireless technology hardware and software will also employ security measures to protect them from viruses, malicious code, and other malware, both known and unknown. As with all CDPH infrastructure components, version updates, bug fixes, and other security-related updates will be kept current and consistent with CDPH policy requirements.

To deploy wireless computing, you will be required to complete a comprehensive security risk assessment and submit that for ISO approval. Risk assessment components include:

- Sensitivity of the information to be transmitted;
- Previous CDPH attempts at wireless computing implementations;
- Statewide implementations of wireless computing;
- Calculation of potential loss to the Department (fiscal as well as reputation);
- Current trends in wireless security standards.

300 Awareness & Training

310 Information Privacy & Security Awareness Training

The CDPH Information Security Policy requires that all employees receive training on this policy and sign acknowledgements of their responsibilities. The CDPH ISO and the Privacy Office will approve training content and schedule mandatory annual Information Privacy and Security Training for all employees.

In addition to CDPH Policy, information privacy and security training is required for all employees by both State and Federal laws and regulations. This includes, but is not limited to:

- State Administrative Manual (SAM) Section 5300.3, Agency Responsibilities, #6, "Maintain a security and ongoing privacy program including an annual training component for all employees and contractors. Refer to Government Code 11019.9 and Civil Code 1798 et seq."
- SAM Section 5325, Human Resources Security, "Each agency is responsible to provide security roles and responsibilities to employees, contractors and third party users. This will ensure the users are informed of their roles and responsibilities for using agency information assets, to reduce the risk of inappropriate use, and a documented process to remove access when changes occur. Personnel practices related to security management must include: #2 Training of agency employees, contractors, and third parties with respect to individual, agency, and statewide security responsibilities and policies."

- HIPAA Security Rule, 164.308(a)(5)(i), "security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management."

400 Audit & Accountability

410 Monitoring System Access

All systems that process, store and/or protect confidential, sensitive, or personal information must create audit logs to identify, at a minimum, the type of event, date and time of the event, subject identity, and the outcome (success or failure) of the event. Each auditable event must be associated with the identity of the user that caused the event (user accountability). Audit logs of system activity are classified as sensitive, and must be secured from manipulation to ensure the integrity of the audit log information.

Audit logs, recording exceptions, and other security-relevant events must be produced and kept for an agreed period to assist in future investigations and access control monitoring. At a minimum, audit logs must include:

- User IDs;
- Dates and times for log-on and log-off;
- Terminal identity or location;
- Records of successful and rejected system access attempts;
- Records of successful and rejected data and other resource accesses attempts;
- Other data elements as required by CDPH.

Procedures must be established for monitoring the use of information processing facilities. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk analysis. Areas that should be considered for monitoring access include:

- User ID;
- Date and time of key events;
- Types of events;
- Files accessed;
- Programs/utilities used;
- All privileged operations (such as, use of supervisor account, system start-up and stop, and input/output device attachment/detachment);
- Unauthorized access attempts (such as, failed attempts, access policy violations, gateways and firewalls, and alerts from proprietary intrusion detection systems);
- System alerts or failures (such as, console alerts or messages, system log exceptions, and network management alarms).

The result of the monitoring activities must be reviewed regularly. The frequency of the review should depend on the risks involved. Risk factors that should be considered include:

- Criticality of the application processes;
- Value, sensitivity, or criticality of the information involved;
- Past experience of system infiltration and misuse;
- Extent of system interconnection, particularly to public networks.

To the greatest extent possible, CDPH must synchronize all system clocks. The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

420 Audit Logs

Access to security audit logs, programs, and utilities must be restricted to those designated by the CISO. Audit logging requirements include:

- The audit trail will trace what happened and who caused it to happen.
- The system will be able to identify a specific individual who has responsibility for any transaction.
- All activities that involve changes to system configuration must be identified, authenticated, and logged so that the specific individual or entity that performed the activity can be identified. Logging must include recording of actions to start and stop logging.
- Each log entry must be date and time stamped.
- Every service start, stop, and refresh must be logged and the initiator identified.
- Access passwords must not be logged.
- All administrator activity and all sensitive system commands must be logged.
- All login attempts, whether completed or failed, must be logged and include the date and time.
- Specified staff, including security, audit, and system administrators, will monitor audit logs periodically.
- Logs must be automatically forwarded to a secure (access restricted to authorized personnel) machine for storage and review, and not stored locally on the source machine or on shared file systems.

430 Log File Retention

It is important to keep records available as long as they are needed for operational, legal, and audit purposes. It is costly and wasteful to keep them longer than required. Where applicable, CDPH must adhere to established legal requirements. The retention schedule must be revised regularly to reflect changes in the law and changes in the Department's forms and procedures.

CDPH audit log file retention periods must be the length of time a record needs to be maintained to satisfy the purpose for which it was created, and to fulfill operational, legal, fiscal, administrative, and prudent business requirements. If log files are needed for legal or approved audit purposes beyond the recommended retention period, retention periods may be exceeded without notice. Shorter retention periods should be considered for logs that are prepared for the purpose of selective audits.

440 Audits

CDPH must allow independent validation of the effectiveness of security measures and ensure that security measures are maintained at planned levels. CDPH must maintain an accurate, up-to-date inventory of all networked devices.

Independent audits of CDPH's information security procedures must be performed at least once each year. Further, independent security audits may review systems that provide access to, or the collection or storage of private information. The audit must verify that all security precautions required by the CDPH ISO as conditions for system approval have been implemented and maintained.

CDPH ISO may remove from service any system that provides access to or stores private information, immediately upon notification by the auditors that essential security measures have not been maintained.

500 Certifications & Security Assessments

510 Vulnerability Assessment Scans

CDPH ISO will establish processes to periodically and independently review the effectiveness of security controls applied to telecommunications and network systems. Vulnerability scanning must be performed on all new or modified systems. Any deficiencies discovered during vulnerability assessment scans must be remediated prior to those systems being placed into production. Only staff authorized by the ISO may perform vulnerability scans. A system must pass all requirements set forth by the ISO and meet minimum requirements as defined in baseline security documents, as well as the Assessment, Certification, and Accreditation process document. Once systems are placed into production, they will be scanned on a continuous basis to ensure they remain in compliance with any Federal, State, or Departmental requirements.

All telecommunications and network systems will be scanned for vulnerabilities by the CDPH ISO at least once a year, or whenever so directed by the ISO.

600 Configuration Management

610 Configuration & Change Management

All new and existing computer and communication systems used for production processing at the Department shall employ a formal change control process to ensure that only authorized changes are made. This process shall include a mechanism for documenting and approving all changes to production computing systems including all significant changes to software, hardware, communications networks, and related procedures.

1. **Hardware, Communications Networks, Operating Systems and Systems Software:** Prior to being installed, new or different versions of hardware, communications networks, operating systems and related systems software for networked production computers shall go through the established change control process.

2. **Application (Executable) Programs:** Executable programs provided by external entities shall be tested successfully before installation on any Department production system. Such testing and examination shall be consistent with Department standards and shall also be properly documented.

3. **Security Fixes:** All security problem fix software, command scripts, and the like provided by operating system vendors, official computer security incident response programs (CSIRPs), and other third-parties shall be tested successfully prior to installation.

620 Unnecessary System Services

Installed services that are unauthorized and not necessary on any CDPH system must be removed or disabled. All applications, components, and services that are not required for the business functionality of the platform must be removed or disabled before the system is placed into production.

700 Disaster Recovery Planning

A Disaster Recovery Plan (DRP) provides for continuity of computing operations in support of critical business functions, minimizes decision-making during an incident, produces the greatest benefit from the remaining limited resources, and achieves a systematic and orderly resumption of all computing services within a Department following a business disruption. A DRP is required for every critical application as set forth in SAM Sections 5355.1 and 5355.2.

The DRP process supports necessary preparation to identify and document procedures to recover critical operations in the event of an outage. Strategies, procedures, and resources must be adapted as often as necessary in order to recover critical applications. Recovery strategies must be developed, tested and updated annually, at a minimum. These strategies should be built from a comprehensive enterprise-wide Business Impact Assessment, which is updated as needed.

To provide for recoverability of new systems, the Department must include disaster recovery considerations and costs in project authority documents and budget proposals. See SAM Section 4900 et seq. and State Information Management Manual (SIMM) Section 20 for requirements and guidelines.

To improve the likelihood for the full recovery of key business processes, DRPs should be developed as part of a complete business continuity program (also know as Continuity of Operations/Continuity of Government – COOP/COG) which includes emergency response and business resumption plans.

It is the responsibility of each program to prepare, test, and update their DRP for each critical and/or time-sensitive application they own. It is the responsibility of the ISO to combine the programs' individual DRPs into a Department DRP, which is in compliance with SIMM Section 65A. The Department DRP must be approved by the Director, or the Director's Designee, and submitted annually to Office of Information Security (OIS) by the required date.

710 Disaster Recovery Management

Disaster Recovery Management includes a Disaster Recovery Plans (DRP). The DRP must be:

- Documented for all critical business functions of the enterprise;
- Based on the results of Business Impact Assessment and risk analysis;
- Documented for the maximum allowable outage (i.e. the recovery time objective) for each identified critical business function;
- Developed in conjunction with both technical and business Program representatives;
- Tested annually;
- Distributed to all individuals who would require them in case of an emergency;
- Kept up-to-date, backed-up by a copy held at an off-site location, and subject to formal change management.

720 System/Data Back-ups

Good business practices for Department systems include daily back-up of that day's activity and weekly back-up of the entire system. Copies of the operating and application system programs, which guide the computer in running the applications, must also be backed up since they are necessary for operating the systems if the originals are damaged or destroyed. It is also important to keep at the emergency alternate site copies of any written procedures and instructions that are needed for computer operators to follow.

730 Off-site Storage

The alternate site used for back-up storage must be close enough to the disaster recovery site so that the back-up data can be delivered to it in a reasonable time, yet at sufficient distance from CDPH to reduce the chances the back-up storage site may be impacted by a regional disaster. Off-site media storage facilities must comply with CDPH policy.

800 Identification & Authentication

810 Authentication

Authentication to access confidential or sensitive information and restricted functions must be assigned and maintained so that the individual person or entity can be uniquely identified. The use of additional authentication processes, including, but not limited to, biometrics, digital certificates, tokens, SecureID cards, or other measures may be employed when required and approved by the Information Owner and the CDPH ISO.

820 Password Authentication

Password authentication must include an identification component (ie., User ID) and a password component. Access to information resources will only be provided if both components are present. The identification component must be a unique alphanumeric combination assigned to an individual. In the case of administrative, system and service accounts, the identification

component is chosen by an Information Custodian. Once established, the identification component for individuals must remain unchanged and be consistent throughout every CDPH information system. The identification component will be retained as long as needed for business or legal requirements.

Employees are responsible for the confidentiality and security of their passwords. The following password protection requirements shall be met to secure data from unauthorized access:

1. Passwords are not to be shared.

2. Select an unusual combination of eight characters or more for a secure password. Avoid words with personal associations, such as names of family members or pets, favorite hobbies, sports, or vacation spots. Non-dictionary words are even more secure.

3. Keep passwords confidential, including passwords used for dial-up access. They are not to be written down, posted where they may be accessed, or included in a data file, log-on script, or macro.

4. Passwords are to be changed immediately if revealed or compromised.

5. Passwords are to be changed every 60 days.

6. Any suspected unauthorized use of a user ID or password is to be reported to one's supervisor and the ISO upon discovery.

Administrative, system and service account passwords must be changed at least annually and when staff having knowledge of, or access to, the password(s) vacate their position. In addition, these types of passwords must always be kept confidential and shared with the minimum number of custodial staff required for system support.

Default passwords, provided with technology products must have the ability to be changed to comply with CDPH policy requirements. The installer or Information Custodian, as part of the installation process, must change the product's default password to some other value before the system is placed into the Department's production network.

900 Incident Reporting & Notification

It is Department policy to maintain a record of security incidents and breaches, and employ security measures that preserve the privacy and prevent the release or destruction of confidential, sensitive, or personal information. This release or destruction may occur through theft, loss, damage, unauthorized destruction or modification, unintentional or inappropriate release, misuse, accident, sabotage or other criminal activity, or natural disaster.

State policy requires Departments to follow specified notification and reporting processes when information security incidents occur. The Department shall adhere to the Information Security Incident Reporting Requirements set forth in SAM Section 5350.1, and the Agency Information Security Incident Notification and Reporting Instructions found in SIMM Section 65B.

An Agency Information Security Incident Report (SIMM 65C) outlining the details of the incident and corrective action to be taken must be completed and forwarded to OIS and CHHSA within 10 business days following the incident. This report must be signed by the Director (or Director's designee) and the Chief Information Security Officer (CISO).

910 Incident Reporting Roles & Responsibilities

Employees: All employees shall immediately report any actual or suspected violations of the Information Security Policy. Once a loss, breach, suspected breach, or violation is discovered, Department employees shall, in the most expedient time possible and without unreasonable delay, report any suspected or confirmed incident to the employee's Division Chief via the employee's chain of command. In the event the employee's Division Chief is unavailable on the day of discovery, the employee shall immediately notify the Information Security Office (ISO) and the Privacy Office.

The employees of the unit in which the incident occurred shall participate in an investigation of the incident with the ISO and Privacy Office, which shall include, at a minimum, interviews of those employees involved in the incident, as well as other witnesses, and review of the business practices that resulted in the incident.

Employees shall also cooperate fully in the investigation, escalation notification and remediation of violations.

Division Chief or Designee: The Division Chief or designee shall immediately notify the ISO and Privacy Office of any actual or suspected breaches or violations of security or privacy policy.

The Division Chief of the unit in which the incident occurred shall ensure that each incident is thoroughly remediated. Remediation of an incident may include changing business practices, providing additional training to employees, discipline of employees, a compliance plan for a business associate contractor, or termination of a contractor.

The Division Chief of the unit in which the incident occurred shall cooperate with the Privacy Office in the drafting and sending of notification letters to individuals whose confidential, sensitive, or personal information is known or suspected to have been obtained by an unauthorized person. Notification letters shall be sent when required under California Civil Code Section 1798.29 or 45 C.F.R. Section 164.400, et seq.and in all other cases when it is the judgment of the Privacy Officer that the confidentiality and integrity of individually identifiable, confidential, sensitive or personal information has been compromised so as to potentially cause harm to an individual.

Chief Information Security Officer: Oversight responsibility to ensure the integrity and security of automated and paper files, databases, and computer systems must be vested in the Department's CISO. The CISO is required to oversee Department compliance with policies, procedures, and incident reporting regarding the security of information assets. The CISO has oversight and responsibility for the Agency Information Security Incident Report (SIMM 65C),

The CISO is responsible for notifying the California Office of Health Information Integrity (CalOHII) for any incident involving attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in

an information system owned by a Health Insurance Portability & Accountability Act (HIPAA) covered entity and containing electronic protected health information (ePHI).

Privacy Officer: The Privacy Officer is responsible for the privacy of all data maintained by the Department, compliance with State and Federal laws regarding privacy and the legally permissible uses and disclosures of confidential, sensitive, or personal information. The Privacy Office is responsible for obtaining complete reports from program units on such incidents, and overseeing and approving corrective action plans to prevent such incidents from occurring in the future.

CDPH Director: The Director has ultimate responsibility for information technology security, privacy, risk management, and disaster recovery planning within the Department. On an annual basis, the Director shall submit an Agency Designation Letter (SIMM Section 70A) designating critical personnel. (See SAM Sections 5315.1 and 5315.2) The Director, or Director's designee indicated in the SIMM Section 70A, must sign-off on every incident and breach notification to the State ISO. Each year, the Director shall certify that the Department is in compliance with State policy governing IT security, risk management, and privacy programs by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM Section 70C). (See SAM Sections 5305 , 5315.1 and 5360)

920 Information Security Violations to be Reported

Criteria for reporting incidents as stated in SAM Section 5350.2 include, but are not limited to, the following:

1. State Data (includes electronic, paper, or any other medium).
    a. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive, or personal. (See SAM Section 5320.5 and Section 160, Information Classification)
    b. Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code Section 1798.29.
    c. Deliberate or accidental distribution or release of personal information by a Department, its employee(s), or its contractor(s) in a manner not in accordance with law or policy.
    d. Intentional non-compliance by the Information Custodian of information within his/her responsibilities. (See SAM Section 5320.3)
2. Inappropriate Use & Unauthorized Access - This includes actions of State employees and/or non-State individuals that involve tampering, interference, damage, or unauthorized access to State computer data and computer systems. This includes, but is not limited to, successful virus attacks, website defacements, server compromises, and denial of service attacks.
3. Equipment - Theft, damage, destruction, or loss of State-owned IT equipment or any electronic devices containing or storing confidential, sensitive, or personal data.
4. Computer Crime - Use of a State information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. (See Penal Code Section 502)
5. Any other incidents that violate Department policy.

1000 Maintenance

To ensure that critical security updates are quickly and effectively applied and to improve operational efficiency, all servers and workstations connected to the CDPH network, and/or which store or transmit CDPH information shall be a part of the CDPH centrally managed system maintenance program.

1010 System Maintenance Policy & Procedures

CDPH must develop, disseminate, review, and update documented information system maintenance policies and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The policy and procedures must be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

1020 Controlled Maintenance

Programs must schedule, perform, document, and review records of maintenance and repairs on information systems in accordance with manufacturer or vendor specifications and CDPH ITSD requirements. Maintenance records for the information system must include:

1. Date and time of maintenance;
2. Name of the individual performing the maintenance;
3. Name of escort, if necessary;
4. A description of the maintenance performed; and
5. A list of equipment removed or replaced (including identification numbers, if applicable).

Programs are responsible for implementing maintenance activities performed on site or remotely, and whether the equipment is serviced on site or removed to another location. Programs are responsible for sanitizing equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and Programs are responsible for checking all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

1100 Media Protection

1110 Media Transport (Mobile Computing & Removable Storage)

For the purposes of this Policy, a mobile computing device is defined as any portable device, such as a laptop, personal digital assistant (PDA), Blackberry, or tablet PC. A removable

storage device includes, but is not limited to, a compact disc (CD), digital video disc (DVD), flash drive, diskette, or other device that has the ability to store information.

Most mobile computing and removable storage devices have the capacity to store Department information. The Department shall ensure due diligence is taken to protect this information appropriately. Employees shall take reasonable precautions for both the security of their mobile computing and removable storage devices, and the information they contain.

1. All mobile and removable storage devices used for Department business purposes are subject to inspection and possible forensic analysis by the ISO or Internal Audits at any time.

2. All mobile computing devices shall meet the Department's hardware and software standards, including data encryption, and be configured with the Department's standard build. Exceptions can only be granted by the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

3. Prior to any non-Department mobile computing and/or removable storage devices being connected to the Department's computer network, approval by the employee's Branch Chief and the ISO is required. Use the Foreign Computer Attach Request Form (CDPH 9058 Form) to request approval. Non-Department mobile computing and/or removable storage devices must also meet all of the requirements set forth in this Policy. Connections are only permitted via approved communication paths. (See Appendix A, Forms Index)

4. Please refer to Appendix C, Information & Data Handling, for handling and protection of classified information.

1120 Media Allocation

1. Regardless of funding source, all mobile computing and removable storage devices issued to individuals remain property of the Department.

2. Upon termination of Department employment, the individual shall return the Department's mobile computing and removable storage device(s) to his or her LAN or IT Administrator, or or their supervisor. This is included on the Exit Clearance Form (CDPH 2005 Form). (See Appendix A, Forms Index)

1130 Media Physical Security

1. Mobile computing and removable storage devices shall not be left unattended at the worksite at any time. When taken off the worksite premises, these devices shall not be separated from employees at airports, automobiles, or hotel rooms.

2. Laptops and tablet PCs used at an assigned workstation shall be cable-locked to an immovable surface, or removed from a docking station and placed in lockable storage whenever the user leaves the workstation.

3. Users shall take precautions to ensure other persons cannot view on-screen data in public locations.

4. The identification number of the mobile computing device shall be recorded and kept separately in a safe place. It shall not be stored with the mobile computing device or in the carrying case.

1140 Media Tracking & Recovery

If a mobile computing or removable storage device is lost or stolen, please refer to Section 900, Incident Reporting and Notification.

1150 Media Maintenance

Employees assigned laptops and tablet PCs are required to update anti-virus applications and system patches monthly. This regular maintenance is accomplished by connecting those devices to the Department's computer network, or by making them available to their LAN Administrators/IT Administrators at least once a month.

1160 Media Sanitization & Disposal

CDPH must mitigate the risk of disclosure when media (magnetic, optical, or other storage methods) is repaired, surplused, surveyed, disposed of, or otherwise removed from the direct control of CDPH.

Computer hard drives include storage devices in desktop PCs, notebook computers, servers, mainframes, network devices, security devices, as well as other digital devices. If a computer contains a hard drive, or other storage device, with confidential, sensitive and/or personal information, the following requirements must be met:

1. If the computer is removed from CDPH for repair, the drive must be "wiped" using the CISO approved utility.

2. If a hard drive is sent outside CDPH for repairs and the unit is not repairable, the vendor must be instructed to return it to CDPH for destruction.

3. If it is necessary to repair the drive in order to restore information which was not backed-up, approval must be obtained from the ISO in order to release the computer for repair.

Prior to disposal of any computer or computer media, the data residing on any drives must be sanitized to eliminate the magnetically recorded data on all drive platters. The most simple degaussing techniques are not sufficient; only ISO approved degaussing equipment may be used. The entity responsible for sanitizing hard drives must perform a minimum of three wipes (using alternating characters as in the Department of Defense Standard - 5200.28-STD) utilizing the software tool approved by the CDPH ISO.

If the wiping process is not able to initiate (system will not boot or recognize the drive) or the process is not able to complete error free, the disk drive must be removed from the device and physically modified or destroyed in such a way as to make the data unrecoverable.

Rapid advances in technology preclude development of a comprehensive policy that specifically identifies all types of storage media. Magnetic positions on specially coated Mylar are no longer the only method of digital storage. Storage devices other than magnetic presently exist and

certainly new devices will be developed. Regardless, the intent is the same--**do not dispose of devices or media that store data unless the information can be certified unrecoverable**.

1200 Physical & Environmental Protection

1210 Physical Security

Physical security policies must be applied, at minimum, to all systems, storage media, and network components. All systems, storage media, and network components that are State-owned or owned by external entities providing CDPH services, must be physically secured so that access is restricted to personnel authorized by the Information Owner. Physical keys to network equipment, (e.g., wiring closets) must be closely controlled and marked "DO NOT COPY". Date, time, and identity must be logged for all access to restricted facilities. These logs are subject to the same retention and review requirements as system audit logs. CDPH must develop and implement a physical security procedures document detailing the measures taken to protect IT assets in the event of disasters (flood, fire, earthquake, explosion, power outage).

The following steps are to be taken to protect computer equipment from theft, unauthorized use, and to ensure that Department systems and information security are not inadvertently compromised:

1. During normal work hours, confidential, sensitive, or personal information shall not be left unattended. If the area will be unattended, even for a few minutes, confidential information shall be locked up in a file cabinet, file room, desk, or office. Unattended means that information is not being observed by an employee authorized to access the information.

2. Visitors to secure areas shall be escorted, and confidential, sensitive, or personal information shall be kept out of sight while visitors are in the area.

3. During non-working hours, confidential, sensitive, or personal information shall be kept in a locked office, desk, file, or cabinet, even if the building is secured.

1220 Environmental & Security Controls

CDPH must consider physical security design standards in the early stages of a facility construction or modification project. Existing or proposed safeguards and recommended security design standards for accommodation must be periodically evaluated against the current threat and risk assessment. CDPH must use security perimeters to protect areas that contain information-processing facilities. Evaluation of a building's architecture for CDPH secure perimeters should be performed to mitigate hidden access points, such as shared walls, raised floors, dropped ceilings, and heating, ventilation and air-conditioning (HVAC) vents. Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. In the selection and design of a secured area, CDPH must consider the possibility of damage from fire, flood, explosion, and other forms of natural or man-made disaster.

CDPH must take into account any security threats presented by neighboring premises, for example, leakage of water from other areas (including other areas within the same facility). Delivery and loading areas must be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

It is important that every computer room be continuously monitored for temperature, smoke, fire, humidity, and water leaks. It is a good practice to alarm (whether by sensors or software) individual pieces of equipment such as computers, servers, data storage devices, network and communications equipment, in addition to the control systems that support the room.

Electrical power must be consistent and reliable, preferably from multiple independent sources. A back-up generator providing back-up power must be specifically designed for this purpose. Battery rooms must be protected against fire and must be temperature controlled for warmth so the batteries do not lose power in cold weather.

1300 Planning

1310 System Security Plan

A system security plan is mandated by the CDPH ISO for all major applications or general support systems, and is applicable to all CDPH employees and contractors. A description of major applications or general support systems, and the requirement for a system security plan can be found within the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", Appendix III, "Security of Federal Automated Information Resources". Additionally, CDPH follows the National Institute of Standards & Technology (NIST) standards. These applicable standards can be found in NIST SP 800-18 "Guide for Developing Security Plans for Federal Information Systems".

The security planning process is a policy requirement applicable to all CDPH employees and contractors. It typically involves project managers, technical staff, and the CDPH ISO. Additionally, some planning activities may need to include program staff, the enterprise architect, the CDPH Privacy Officer, and/or the CIO.

The security plan is a mandatory document for all IT systems unless the CDPH ISO has granted an exception. The security plan must be approved by the ISO prior to system implementation. The ISO will not approve change controls for systems without an associated, approved security plan.

1400 Personnel Security

1410 Security & Confidentiality Acknowledgements

Before granting physical or system access to CDPH information resources, all Information Users are required to sign the Security and Confidentiality Acknowledgment (CDPH 2420 Form). Thereafter, this Security and Confidentiality Acknowledgement must be reviewed and renewed annually by re-signing. Managers and supervisors shall maintain signed acknowledgments in their unit files for all employees using, or otherwise having access to, Department information. (See Appendix A, Forms Index)

1420 Access Agreements

Before granting physical access or disclosing CDPH confidential, sensitive or proprietary information to third parties such as contractors, vendors or business partners, the individual and officer of the recipient organization must sign a CDPH-approved agreement or exhibit and the transaction must be approved by the Information Owner and the CDPH ISO and/or Privacy Officer.

1430 Separation and Transfers

In the event that an employee separates from the Department (voluntary or involuntary), or transfers within the Department, the employee's immediate supervisor is responsible to:

1. Complete and submit the employee's Exit Clearance Form (CDPH 2005 Form).

2. Ensure all physical property in the custody or control of the employee including, but not limited to, keys, identification cards, software, mobile computing devices, removable storage devices, data and documentation, is returned in good condition before the employee separates or transfers within the Department. If such property is not returned, or is not returned in good condition, ensure that appropriate Department personnel management is informed.

3. Notify the LAN Administrator/IT Administrator that all privileges associated with the employee's user ID must be revoked.

4. Terminate all other work-related privileges of the employee at the time that the separation or transfer takes place.

1500 Risk Assessment

1510 Risk Management

Risk management is the process of taking actions to avoid or reduce risk to acceptable levels. This process includes both the identification and assessment of risk through risk analysis (SAM Section 5305.1) and the initiation and monitoring of appropriate practices in response to that analysis through the Department's risk management program.

The Department must ensure the integrity of both paper and electronic information resources by protecting them from unauthorized access, modification, destruction, or disclosure and to ensure the physical security of these resources. The Department shall also ensure that users, contractors, and third parties having access to Department information resources are informed of, and abide by, this policy (SAM Section 5305).

1520 Risk Analysis

Risk analysis is an essential aspect of the IT security and risk management program. The Department shall establish a risk analysis process to identify and assess risks associated with

the IT assets, and define a cost-effective approach to managing such risks. Specific risks that shall be addressed include, but are not limited to, those associated with accidental and deliberate acts on the part of Department employees and outsiders; fire, flooding, and electric disturbances; and loss of data communications capabilities.

The risk analysis process must identify and prioritize critical applications of information technology. When establishing priorities, the Department should consider that applications may become more critical as the period of unavailability increases and that processing cycles (i.e., monthly, quarterly, or yearly) may have an impact upon the prioritization of applications. The Department's risk management practices and disaster recovery planning must give priority to the establishment of policies and procedures to ensure the continued operation of these applications (SAM Sections 5310 and 5355).

The risk analysis process shall be carried out with sufficient regularity to ensure that the Department's approach to risk management is a realistic response to the current risks associated with its information assets. In general, the risk analysis process is a cyclical process. The Department shall complete the comprehensive risk analysis cycle at least every two years, and whenever there has been a significant change in the use of information technology. This cycle ends with the preparation of a report documenting the risk assessment.

The risk analysis process shall include the following:

1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and program management.

2. Identification of the Department's information assets that are at risk, with particular emphasis on the IT applications that are critical to the Department's program operations. A critical application is defined as an application that is so important to the State that the loss or unavailability of the application is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or State employees; on the fiscal or legal integrity of State operations; or on the continuation of essential Department programs.

3. Identification of the threats to which the information assets could be exposed.

4. Assessment of the vulnerabilities. For example, the points where information assets lack sufficient protection from identified threats.

5. Determination of the probable loss or consequences, based upon quantitative and qualitative evaluation, of a realized threat for each vulnerability and estimation of the likelihood of such occurrence.

6. Identification and estimation of the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level;

7. Selection of cost-effective security management measures to be implemented; and

8. Preparation of a report, to be submitted to the CDPH Director and to be kept on file within the Department, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of remaining risk to be accepted by the Department.

1600 System & Services Acquisition

1610 Software Licensing, Copyrights & Intellectual Property

Intellectual property (such as computer software and other digital content) must be used in a manner compliant with applicable copyright laws and licensing agreements. CDPH expressly forbids the installation or copying of intellectual property on CDPH owned or managed information resources without the approval of CDPH management and the ISO.

Open source and other types of free software (including plug-ins and applets, etc.) may not be loaded on any CDPH information resource without the approval CDPH management and the ISO.

1620 Technical Documentation

The centralized IT Division will develop and maintain current and accurate documentation for all telecommunications, network, and information systems. This includes, but is not limited to: standards, procedures, operating system configurations, all installed software, service packs and patches, firmware versions, detailed network diagrams, program source code, Job Control Language specifications, data definitions, etc.

Technical documentation will be maintained in a secure manner and authorized individuals with the need to know. Should documentation need to be shared with other entities (i.e., for projects, presentations, etc.), it may be necessary to redact critical security information from the documentation (for example, specific IP addresses; firewall, server or router configurations; administrative system accounts; etc.).

1700 System & Communications Protection

1710 Firewalls

All connections between the Department's internal networks and the Internet (including other State agencies or any other publicly accessible computer network) shall include an approved firewall or related access control system. The privileges that will be permitted via this firewall or related access control system will be based on Department business needs.

1. All firewalls shall be maintained by the centralized IT Division.

2. All firewalls used to protect the Department's internal network shall run on separate dedicated computers. These computers shall not serve any other purposes (such as acting as web servers).

3. Firewall configuration rules and permissible service rules shall not be changed without following formal Change Management Procedures and prior approval of the ISO.

4. Firewall configurations shall be periodically checked to ensure that they have not changed during software modifications or re-booting of equipment.

1720 Telecommunications & Network Security

Information Owners and Information Custodians of all CDPH systems, with the review and approval of the CDPH ISO, must restrict those functions and processes that can be misused to compromise the security or availability of systems and information. These functions and processes may include, but may not be limited to, any applications, system functions, utilities, transactions, or information that can be misused to compromise the confidentiality, integrity, or availability of CDPH information or systems, or to disable security protections.

Effective system access controls must be established and maintained to:

1. Present an approved warning banner each time a user attempts access to any CDPH computer system, regarding the confidentiality of the data in the system and the consequences for unauthorized access and use. The user must acknowledge and accept the terms and conditions of the banner prior to system access. The acceptance of the acknowledgement must be logged. (See Appendix E, Sample CDPH Warning Banner)

2. Restrict access to confidential information to individuals authorized by the Information Owner. Access to such information must be provided upon the specific identification and authentication of the individual.

3. Control access to restricted functions. All such access must be provided upon the specific, individual identification and authentication of the person or entity. Accountability shall be maintained for all access to system resources through audit trails of employee activity.

4. Immediately disable authorization to perform functions or obtain information upon notification of compromise.

5. Automatically disable accounts used for authentication after three unsuccessful logon attempts. Access may be manually or systematically restored after a predetermined time period.

6. Configure workstations, servers and other personal computing devices to automatically lock system access if unused for ten (10) minutes. Users must have the capability to manually lock the system without logging off.

Users must be granted rights and privileges only on a "need to know" or only on a need-to-use basis and according to the *principle of least privilege.* When system users have elevated privileges (such as, LAN, IT and Database Administrators) they must consider the access control requirements contained herein as minimum standards. Where possible, these Administrators must employ more stringent access control measures.

1730 Encryption

Encryption involves the altering of data objects in a way that the objects become unreadable until deciphered. All CDPH encryption (data in transport and at rest) must conform to Federal Information Processing Standards (FIPS) 140-2. When using public/private cryptographic keys, a CDPH ISO approved solution must be used to distribute the keys. Cryptographic keys must have defined activation and deactivation dates so they can only be used for a limited period.

The cryptographic keys will adhere to the following standards:

- Private keys must be kept confidential.
- Key management must be fully automated.
- Use a short life for cryptographic keys. Keys with a long life must be used sparingly.
- Encryption will be used to protect keys in storage and transit. No key can appear in the clear outside a cryptographic device (i.e., an RSA token).
- Keys must be randomly chosen from the entire key space.
- Key encrypting keys must be separate from data keys. Keys that are used to encrypt other keys must not be used to encrypt data, and vice versa.

1740 Communications Methods/Data Transmission

Any information sent over the Internet or other unsecured communication lines can be intercepted and read, modified, or otherwise corrupted. Therefore, all information classified as confidential, sensitive or personal must be encrypted (using the ISO approved encryption solution) during information/data transport on all public telecommunications and network systems, and at all points not in the direct ownership and control of the Department.

In performing Department business, all employees shall take every precaution to ensure the security and privacy of the information. Confidential, sensitive, or personal information may be transmitted via Internet and/or E-mail only when:

1. Program management approvals have been obtained; and

2. Encryption, authentication, and/or any other ISO approved security schemes and/or policies are used to ensure that data is secured and made available to appropriate and intended recipients only. (See Section 1730, Encryption)

Streaming media and teleconferencing, including PC cameras and microphones, will employ security measures to protect them from inadvertent disclosure of information due to corruption, misdirection, diversion, or interception. The security precautions will be kept current with the evolving technologies for streaming media and teleconferencing hardware and software.

Modems may be installed on a CDPH system only with the prior approval of the ISO. When modems are allowed, they must only be permitted when connected to properly secured and hardened systems. CDPH ISO will monitor hardware configurations through audits by use of ISO approved tools to determine if unauthorized modems exist within the CPDH computing environment. CDPH is required to periodically change modem dial-up access telephone numbers.

1800 Security & System Integrity

1810 Patch & Vulnerability Management.

The purpose of this policy is to provide direction for managing the implementation of information security patches, hot-fixes and updates. Patches, hot-fixes and updates are routinely created

and published by various hardware and software vendors to correct potentially serious security and reliability flaws.

1. LAN Administrators/IT Administrators shall apply all vendor recommended bug fixes, service packs and security patches on operating systems, applications, and/or hardware appliances as prescribed by the patch application process defined by the IT Division.

2. The IT Division will monitor relevant security issues, both internally and externally, and will manage the release of security patches on behalf of the Department.

3. The IT Division will work with appropriate LAN Administrators/IT Administrators to test security patches before release, where practical.

4. Security patches shall be implemented within the timeframe specified by the IT Division.

Systems deemed non-compliant will be reported to the ISO as being vulnerable. The ISO, upon agreement with the CIO, will determine whether the system should be removed from service until the patch, hot-fix, or update has been applied, or until an implementation plan has been reviewed and approved by the ISO.

1820 Server Configuration & Hardening

To ensure that critical security updates are quickly and effectively applied and to improve operational efficiency, all servers and workstations connected to the Department network, and/or which store or transmit Department information shall be a part of the IT Division centrally managed system management program. All servers shall adhere to ISO approved server configuration and hardening standards.

1830 Hardware/Software Upgrades

1. Only authorized employees are permitted to perform system upgrades (e.g., LAN Administrators/IT Administrators, approved IT personnel).

2. All system upgrades (e.g., servers, routers, firewalls, software, etc.) shall adhere to the Change Control Policy. (See Section 610, Configuration & Change Management)

1840 Application Development

Information processing and communications applications must be designed, developed, and enhanced to ensure their reliability. Based on the *principle of least privilege*, applications being developed, tested and maintained at CDPH must function properly with the user of that application having the lowest level of operating system privileges on the local workstation.

Developers of information systems, including entities providing contract services, must implement the security controls specified by the Information Owner and the CDPH ISO; integrate procedural safeguards for the information resources; assist Information Owners in evaluating the effectiveness of security controls and exception reporting; and implement the techniques and procedures for detecting, reporting and investigating breaches in Information Security.

1850 System Testing & Training

CDPH must maintain test environments for systems that provide access to or store confidential information. All new or modified software must be sufficiently tested to ensure the integrity of the information, and the results approved by the CDPH ISO before being installed on production systems. Changes to CDPH services need to be documented, and all documentation must be available to operational, security, and audit personnel. During system testing and training of system users, no production, confidential, sensitive or personal data may be used without prior management approval.

1860 Virus Protection

All CDPH computer workstations and laptops must have anti-virus software installed and resident in memory at all times, and must have the manufacturer's most recently available virus definition file, loaded, and in use by the anti-virus software.

The anti-virus software must be configured to:

- Start upon system boot-up (as a service where possible);
- Detect and clean viruses, worms, Trojan horses, and other malicious code;
- Scan and clean incoming and outgoing electronic mail (as applicable);
- Block script-based threats;
- Allow for automatic updates;
- Scan all files introduced to the computer;
- Prevent the user from disabling the product.

Anti-virus software must also be installed on all CDPH servers, including systems hosting user files and systems running critical applications.

One of the main virus delivery methods continues to be by way of Internet E-mail attachments. Therefore, CDPH Internet E-mail users must exercise extreme caution when opening all message attachments, particularly when received from an unfamiliar source. If in doubt, contact CDPH IT Service Desk (800-440-7000).

1870 Workstation Security

Employees are responsible for the security of their assigned Department resources and the information under their control. The following steps are to be taken to protect computer equipment from theft, unauthorized use, and to ensure that Department systems and information security are not inadvertently compromised:

1. Employees shall use Department information and resources only for Department business purposes.

2. Employees accessing Department information assets shall use due care to preserve data integrity and confidentiality. (See Section 150, Information/Data Policy)

3. Employees shall not possess, or attempt to obtain, a network protocol analyzer or similar device (including software) for capturing and/or reading electronic signals from the State's computer network, without prior approval from the ISO.

4. Employees shall not possess, or attempt to obtain, password-breaking software (e.g., crack) used to guess employee passwords without prior approval from the ISO.

5. Employees shall not intentionally destroy, modify, or release computer programs or data, or introduce malicious code (such as a computer virus).

6. Desktop systems shall be kept in secure areas (i.e., a secure building or room) or shall be physically attached to a desk or table.

7. The use of surge protectors is required.

8. Unattended PCs shall be protected with a password protected screen saver.

9. Employees are not authorized to turn off or disable virus-checking systems. Employees shall scan all diskettes or other media for viruses prior to use.

10. Employees shall complete annual training about the Department's information security policies, and sign acknowledgments of their security responsibilities. (See Section 300, Awareness & Training, and Section 1400, Personnel Security)

11. Once confidential, sensitive, or personal information has met designated retention periods, it shall be disposed of through confidential means (shredded, pulverized, etc.) with the destruction being witnessed by a State employee. Confidential, sensitive, or personal information ready for destruction shall not be stored in boxes in employee's cubicles or offices. Such information shall be deposited in locked, confidential destruct bins or shredded on-site. (See Appendix C, Information & Data Handling)

1880 Malicious Mobile Code

Mobile code (also called Active Content) is technology that allows for the creation of executable information that can be delivered to an information system and directly executed on any hardware/software architecture that has an appropriate host execution environment. Its use is widespread and increasing in both commercial and government applications. Mobile code has the potential to severely impact CDPH operations if not monitored, or if used improperly. The CDPH must maintain malicious code protection software and periodically perform scans for the existence of malicious code on any CDPH computer or server.

CDPH will maintain procedures for the mitigation of malicious mobile code. These procedures must include provisions to ensure that updates to malicious code protection software are applied on all CDPH systems within one week of general availability. CDPH will document and report incidents of malicious code discovered on systems and networks to the CDPH ISO.

In order to identify potentially hostile code before it can enter the CDPH network, mobile code must be stopped and inspected at the firewall or gateway, away from critical resources. CDPH must prohibit execution of code that has the potential to compromise the performance or security

of CDPH computer systems. This includes, but is not limited to, code that may change system configurations, delete or corrupt data, or take control of client machines.

Mobile code monitoring must include the creation of detailed log files. The log files must record both system events and user events. The log files must be saved for a minimum of 90 days, stored electronically, and made available to the ISO. Furthermore, mobile code monitoring must have the capability to send automatic E-mail notifications (alerts) upon the detection of hostile mobile code.

1890 Intrusion Detection & Prevention

CDPH must record, review, and analyze unauthorized attempts to access CDPH computer systems. A combination of three basic methodologies to detect intrusion must be used: 1) audit trail analysis (host monitoring), 2) packet analysis (network monitoring), and 3) real-time activity monitoring.

Any available information regarding the identity of the entity attempting access and the nature and extent of the access must be logged.

CDPH must develop a plan to respond to detection or external notification of attempts at unauthorized access to CDPH computer systems. This plan shall be compliant with Section 900, Incident Reporting and Notification Procedures, of this policy and must include specific assignment of tasks to individuals or organizational entities and establish time-based escalation processes.

CDPH must implement automated or manual processes to:

- Log and analyze changes to the system configuration or performance that may cause or indicate security threats or vulnerabilities.
- Review intrusion detection system logs to identify attempts to gain unauthorized access to private information.
- Provide real-time notification to incident response personnel of unauthorized access to system level functions and anomalous telecommunications and network activities.

CDPH must periodically test the intrusion detection infrastructure, including the Incident Reporting and Notification Procedures document, to verify its effectiveness and performance are in conformance with intrusion detection plan objectives. In addition, the CDPH must periodically review the response to actual incidents to provide for continuous improvement of CDPH's intrusion detection posture.

CDPH must establish and maintain automated or manual processes to provide real time notification of unauthorized access to system level functions that can potentially alter the security processes on CDPH systems providing access to confidential information. CDPH must establish procedures for the analysis and reporting of anomalous activity.

Network activities must be logged and analyzed to identify changes to network configuration or performance that may cause or indicate security threats or vulnerabilities. CDPH must establish procedures for the logging, analysis, review, and reporting CDPH network activities. The CDPH must have in place mechanisms for the real-time identification and reporting of anomalous network activities.

1900 Acceptable Use of Information Technology Resources

This policy applies to employee's having access to, or use of, Information Technology (IT) resources owned, operated, or managed by CDPH or the State of California. This policy applies to the use of IT resources from remote locations (e.g., while teleworking) as well as from a CDPH worksite.

All employees must adhere to their roles and responsibilities (as detailed in Section 140), follow the Information Security Policy, complete the annual Information Privacy and Security Awareness Training, and read/sign the Security and Confidentiality Acknowledgement (CDPH 2420 Form). (See Appendix A, Forms Index)

Department employees are granted access to IT resources to provide education, research, marketing, procurement, and service opportunities in the performance of their duties. These resources are provided to conduct State business and are routinely monitored for improper use. Anyone using these resources expressly consents to such monitoring. Employees who access IT resources are to follow these guidelines, unless an exception has been granted by the employee's supervisor in writing and the access/use is required for the employee to conduct official Department business.

All employees shall:

1. Conduct all Internet and/or E-mail activities in a professional, lawful, and ethical manner, including the use of and development of content for the Internet.

2. Support the use of existing infrastructure, technologies, procedures and standards in using, developing, or making information available on the Internet.

3. Be restricted from participating in mailing lists, discussion groups, newsgroups, list servers, or other interactive communications if such participation is excessive or is inhibiting overall network performance.

4. Comply with this policy when conducting State business even when accessing a personal or private Internet Service Provider. This includes both State and non-State equipment.

The intentional use of State time and resources for personal advantage, gain, or profit is inconsistent, incompatible, and in conflict with the duties of officers, contractors, and employees of the Department and is prohibited. Examples of such inappropriate use include, but are not limited to, viewing, sending, creating, and/or downloading any information that:

1. Violates or infringes on the rights of any other person or entity, including the right to privacy.

2. Contains defamatory, false, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.

3. Violates State laws or Department policies prohibiting sexual harassment and discrimination.

4. Restricts or inhibits other users from using the system or the efficiency of the computer systems, unless such restriction or inhibition is expressly provided for in this Policy.

5. Encourages the illegal use of controlled substances.

6. Utilizes the system for any other illegal purpose.

Employees also shall not use the facilities and capabilities of Department resources to:

1. Conduct, engage, or solicit the performance of any activities in violation of any State, Federal or local laws, regulations, rules, executive orders, agency or Department regulations, policies or directives.

2. Transmit material, information, or software in violation of any local, State or Federal law.

3. Conduct any political activity.

4. Conduct any unapproved fundraising or public relations activities.

5. Operate a personal Web Server or make available any Internet services using such server.

6. Engage in any activity for personal gain or personal business transactions.

7. Make any unauthorized purchases.

8. Use Department records for private gain, or divulge confidential Department information or records unless officially authorized to do so.

9. Attempt access to information resources without authorization and a business need.

10. Install or connect unauthorized software or hardware on CDPH owned and/or managed information systems.

11. Store personal or non-business related data and multi-media files on CDPH servers or other centrally managed resource.

1910 E-mail Messages & Instant Messages

E-mail messages and instant messages (IM) distributed via the E-mail and IM systems are CDPH property and not the private property of individual users.

E-mail and IM systems must not be used for:

1. Automatic forwarding of E-mail messages to external recipients.

2. Transmitting classified information to external recipients unless encrypted with a method approved by the CDPH ISO and appropriate to the employee's job duties and responsibilities.

3. Circulating chain mail, jokes of the day, non-business related video clips, and digital images.

4. Distributing religious, political, sexual, or offensive content.

1920 External E-mail & Instant Messaging

While connected to the CDPH network, the use of external E-mail and IM services (e.g., your home E-mail and IM accounts) are prohibited unless approved by the CDPH ISO.

1930 File Sharing

State and Federal law prohibits the unauthorized transfer or sharing of music, movies, software, and other intellectual property. Therefore, unauthorized use of peer-to-peer (file sharing) software is prohibited at CDPH. Peer-to-peer technologies must be approved by the CDPH ISO for business use.

Appendix A: Forms Index

The following is a listing of forms referenced in the CDPH Information Security Policy. They are in numerical order by form number. There is also a brief description of each form. These forms can be found on the CDPH intranet and on the ISO webpage:
http://cdphintranet/technology/ISO/Pages/InformationSecurityForms.aspx

1. CDPH 2005 Form, **Exit Clearance Form** – Used by a manager/supervisor every time an employee separates (voluntarily or involuntarily) from CDPH, or transfers within CDPH.
2. CDPH 2375 Form, **Breach/Incident Reporting Form** – Used whenever there is a security incident such as a lost Blackberry, stolen laptop, or paper document breach.
3. CDPH 2420 Form, **Security & Confidentiality Acknowledgement** – Signed by a CDPH employee, contractor, or temporary employee to acknowledge that they are aware of, and will comply with, the Information Security Policy and procedures. This is required to be signed annually, and managers/supervisors should maintain a file with signed forms for all employees that report directly to them.
4. CDPH 2434 Form, **Exception Request for Content Filter Special Access** - Used to request an exception to a filtered Internet website. Sometimes referred to as a Websense Exception Request.
5. CDPH 2442 Form, **Remote Access Authorization Request** – Used to create, modify or delete Citrix access. Sometimes referred to as a Citrix Request.
6. CDPH 9058 Form, **Foreign Computer Attach Request** – Used to request an ISO exemption PRIOR to attaching any non-CDPH computer to the network. Please attach completed form in an E-mail to cdphinfosec@cdph.ca.gov.
7. CDPH 9069 Form, **Variance Request Form** – Used to request an ISO exemption PRIOR to implementing a solution contrary to an established policy, procedure, guideline, or requirement. Please attach completed form in an E-mail to cdphinfosec@cdph.ca.gov.
8. **Extranet Team Collaboration Request Form for Sharepoint** - Use this form to request collaboration with the ITSD team to create an Extranet Sharepoint website. Create a Remedy ticket and attach the completed form to route to CDPH.
9. **Investigations Request Form** - Used to request an Information Security investigation related to suspected violation of CDPH policy (such as inappropriate computer use). Division Chief or above must attach completed form and send an E-mail to cdphinfosec@cdph.ca.gov and mark as "Private". Due to the confidentiality of these requests, **do not** send them through Remedy.
10. **SFTP Authorization Request** – Used to request SFTP sites for secure transfer methods.

Appendix B: Glossary

Authentication	A process of confirming the correctness of the claimed identity. Authentication is often a prerequisite to allowing access to network resources.
Critical Application	Defined in SAM Section 5305.1, as an application that is so important to the State that the loss or unavailability of the application is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or State workers; on the fiscal or legal integrity of State operations; or on the continuation of essential agency programs.
Encryption	Cryptographic transformation of data (called "plain text") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.
Firewall	A network device or collection of devices that protect inside "trusted" networks from external "untrusted" networks, such as the Internet, using a variety of technical processes.
Information Custodian	The person responsible for overseeing and implementing the necessary safeguards to protect the information assets, at the level classified by the Information Owner. Most times, this would be an IT Administrator, System or Network Administrator, LAN Administrator, Database Administrator or other IT support person.
Information Owner	The person or program that creates, or initiates the creation or storage of the information, is the Information Owner. Within CDPH, if a program is the Information Owner, then the person responsible for that program is designated responsible. The Information Owner is responsible for classifying information appropriately, authorizing access is appropriately, and that safeguards are taken, as necessary. The Information Owner should create and maintain an inventory of all classified information.
Information User	Any person who views, amends, or updates the content of the information assets. Within CDPH, this would be all employees, contractors and student assistants that have access to Department information.
Integrity	The need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
Internet & E-mail Resources	Include employees, hardware, software, and supporting infrastructure.
Mobile Computing Device	Includes, but is not limited to, any portable device, such as a laptop, personal digital assistant (PDA), Blackberry, or tablet PC.

Network Activity	Personal computers, data packets, electronic files, printed materials electronic mail, data records, website communication, password sharing, software, hardware, modem or any other related items or functions performed using State property or conducting State business.
Network Protocol Analyzer (also known as a network analyzer, packet analyzer, or sniffer):	Computer hardware or software that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and eventually decodes and analyzes its contents according to the appropriate RFC or other specifications.
Principle of Defense in Depth	Layered security mechanisms increase security of the system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system
Principle of Least Privilege	A user or program must have access to information or resources that are necessary to complete its task or assignment.
Principle of Separation of Duties	This is the concept of having more than one person required to complete a task. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users. This principle is demonstrated in the traditional example of separation of duty found in the requirement of two signatures on a check.
Proxy Server	A server that acts as an intermediary between a workstation user and the Internet so that the Department can ensure security, administrative control, and caching service. A proxy server is associated with, or part of, a gateway server that separates the Department's network from the outside networks, and a firewall server that protects the Department's network from outside intrusion.
Political Activity	Activities pertaining to campaigning for public office or campaigning on behalf of other candidates running for public office in partisan and nonpartisan elections; contributing money or services to political candidates or organizations, or organizing political fundraising functions or activities; using official authority or influence to interfere with or affect the results of an election or nomination.
Removable Storage Device	Includes, but is not limited to, a compact disc (CD), flash drive, diskette, tape or other removable devices that have the ability to store information.
Workstation	Sometimes referred to as personal computer (PC), laptop computer, notebook computer, tablet PC, etc.

Appendix C: Information & Data Handling

Safeguards for Handling Classified Information

Specific required procedures exist with regard to the physical safeguarding of confidential, sensitive, or personal information. Employees handling this type of information will:

1. Store files and documents containing this information in locked file cabinets. If necessary, confidential, sensitive, or personal information may be stored unlocked in a locked/secured room or storage system.

2. Keep confidential, sensitive, or personal information locked in an office, desk or cabinet during non-working hours.

3. Limit employee access to confidential, personal, and sensitive information to alleviate unnecessary access to files; which should be accessed on a "need to know" basis.

4. Dispose of confidential, sensitive, or personal information in locked confidential destruct bins or containers, which are clearly marked as "Confidential".

5. Dispose of confidential, sensitive, or personal information through secure and confidential means (shredded, pulverized, etc.) once the information has met its designated retention period. A State employee shall witness disposal.

Removal of Classified Information

When removing confidential, sensitive, or personal information from a Department facility:

1. Ensure that all records containing confidential, sensitive, or personal information are inventoried before they are removed from a Department facility.

2. Employees shall not discard confidential, sensitive, or personal information on their own and shall return all confidential, sensitive, or personal information to their Department offices for confidential destruction.

3. Employees shall not store confidential, sensitive, or personal information in home or private storage units, for extended periods of time.

4. Employees shall not leave confidential, sensitive, or personal information unattended at any time in vehicles.

5. Employees shall not check confidential, sensitive, or personal information in baggage on commercial airplanes. If boxes of such documents need to be transported to remote locations, they should be sent via a secure, bonded courier with a tracking system.

6. During closure of an office or move, managers and supervisors shall ensure that security of confidential, personal, and sensitive information is maintained.

Faxing Classified Information

1. Managers and supervisors shall ensure employees are assigned to regularly check for faxes containing confidential, sensitive, or personal information, place the fax in a manila folder to protect confidential, sensitive, or personal information, and deliver to the addressee in a timely manner.

2. Fax machines shall be placed away from potential access by the public.

3. When sending faxes, employees shall notify the recipient that a document is being faxed, verifying the fax number at the time.

4. Employees shall not leave faxes unattended.

5. Managers shall ensure that their unit(s) has a designated fax machine for sending and receiving faxes containing confidential, sensitive, or personal information.

6. Employees shall add a confidentiality statement at the beginning or end of every fax that contains confidential, sensitive, or personal information notifying persons receiving the fax in error to contact the sender and destroy the document.

Mailing Classified Information

1. Employees shall verify the address before sending correspondence that contains confidential, sensitive, or personal information.

2. Employees shall ensure that the address on the envelope has been accurately transcribed, that outgoing correspondence containing confidential, personal, or sensitive information is placed in an envelope so that the information is not visible, and that the inside address and address on the envelope match.

3. Employees and managers shall ensure that transportable media (disks, CDs, cassettes, USB drives, and all other removable storage devices) containing confidential, sensitive, or personal information are encrypted when sent or received through the mail. Such media shall be mailed through a secure bonded courier with tracking or return receipt and signature required.

4. Employees and managers shall ensure that incoming correspondence marked "confidential", "sensitive", "personal", or with like descriptions indicating it should remain private, is delivered unopened to the intended recipient.

5. Employees and managers shall regularly update directories and client databases with current contact information (including databases of contractors).

Oral Communications of Classified Information

1. Employees shall take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential, sensitive, or personal information, regardless of where the discussion occurs (telephone, restrooms, break rooms, etc.)

2. Employees shall find enclosed offices and/or interview rooms for the verbal exchange of confidential, sensitive, or personal information, where possible.

3. Managers shall promote employee awareness of the potential for inadvertent verbal disclosure of confidential, sensitive, or personal information.

4. Employees shall verify the identity and authority to access the information of the person to whom the employee is verbally exchanging confidential, sensitive, or personal information.

5. Employees shall ensure the verbal exchange is an authorized disclosure of confidential, sensitive, or personal sensitive information.

Storage of Classified Information

1. Records containing names, social security numbers, medical or financial information shall not be downloaded or stored on mobile devices unless absolutely necessary for program operations.

2. In cases where use of mobile devices for downloading or storage of confidential, sensitive, or personal information has been determined to be absolutely necessary, the following criteria shall be met:

    a. Only the minimum amount of confidential, sensitive, or personal information necessary shall be downloaded or stored.
    b. The information shall be encrypted.
    c. Social security numbers shall not be associated with names on mobile devices, if at all possible.

Destruction of Classified Information

In cases where downloading or storage of information classified as confidential, sensitive, or personal information has been determined to be necessary, the following deletion/destruction methodology shall be used:

1. Employees are required to delete classified information from their devices if it is clearly no longer needed or potentially useful. Use of an "erase" feature (e.g., putting a document in a virtual recycle bin) is not sufficient for classified information because the information may still be recoverable. Classified information shall be deleted via an overwrite (zeroization) program, degaussed and/or physically destroyed prior to disposal. (See Section 1160, Media Sanitization & Disposal)

2. Prior to disposal, media (e.g., floppy disks, CDs, DVDs, flash drives, tape or other removable media) containing classified information shall be degaussed or deleted via an overwrite program. This includes defective or damaged media. (See Section 1160, Media Sanitization & Disposal)

3. Other storage media, such as paper, containing classified information shall be disposed of in the locked destruction bins located in Department offices.

Appendix D: CDPH Social Networking Guideline

Purpose: CDPH allows access to some social networking sites. These Guidelines provide the necessary parameters that employees must follow if they need to engage in access to, or use of, social networking sites for Department business related purposes. For the purposes of this guideline, social networking includes, but is not limited to, blogs, wikis, message boards, online social networks or communities (e.g., MySpace, FaceBook), or any other form of online publishing or discussion.

Background: The popularity of social networking sites such as MySpace, Facebook, Twitter and others has exploded in recent years. These sites are popular not only for personal purposes, but CDPH, as well as other government agencies and private organizations, have come to realize the benefit these media offer in communicating with their customers. While there are many positive aspects of using social networking sites, it is also important to understand the potential security and other risks in doing so, and to know what precautions you must take to protect the Department, yourself, and your personal or CDPH-related information.

Role & Responsibility: The following items discuss your general responsibilities and obligations. Failure to abide by these guidelines can result in an adverse employment action.

- Read, understand and follow the CDPH Internet/Electronic E-mail Policy, Health Administrative Manual (HAM), Section 6-1010.4
- Be aware that CDPH has systems in place that allow internet usage to be logged and tracked. The Department does not routinely monitor social networking sites. However, as with other electronic resources, CDPH systems administrators may perform activities necessary to ensure the integrity, functionality and security of the Department's electronic resources. Also be aware that other employers, organizations, and individuals do monitor and share information they find on social networking web sites. Posted information is public information.
- In response to concerns, complaints and/or information provided by individuals, Department computer administrators may look up profiles on social networking sites and may use the information in informal or formal proceedings.
- Misuse or abuse of internet access is a direct violation of the CDPH Internet/Electronic E-mail Policy, HAM Section 6-1010.4.
- Access to social networking sites is for business related purposes only. Employees are not permitted to access social networking sites to check or update personal social networking sites, or to view social networking sites of friends or acquaintances.
- Please refrain from clicking on advertisements that may be found on social networking sites. Many times these advertisements contain active content that may have malware embedded in them. By clicking on advertisements the potential exists that malware may be loaded on to your system that could cause a security incident.

- Social Networking sites that are acceptable to visit are those that are maintained by government agencies or private organizations used to communicate business related information that has a direct correlation to your specific job function.
- When using Department electronic resources to access on-line social networks, employees must act with honesty, integrity, and respect for the rights, privileges, privacy, sensibilities, and property of others. Employees must abide by applicable laws, including copyright, trademark and fair use laws.

- Do not expose and/or share confidential or other CDPH proprietary information.
- If you are considering asking to have material posted, consider the image you want to portray to the public. Be mindful that what you post may be viewed by business partners, your peers, supervisors, community members, and may stay public for a long time.
- Remember, there may be consequences to what you post. Consider your content carefully. If you are about to post something that makes you even the slightest bit uncomfortable, review these guidelines first. If you still are uncertain about whether to post the material, check with your manager/supervisor.
- Employees or groups within the Department are not permitted to present personal opinions in ways that imply endorsement by CDPH. If posted material may reasonably be construed as implying the support, endorsement, or opposition of CDPH with regard to any personal statements, including opinions or views on any issue, the material shall be accompanied by a disclaimer. The disclaimer is an explicit statement that the employee/group is speaking for himself/herself, and not as a representative of CDPH or any of its offices or units. An example of a disclaimer is as follows:

  > The contents, including all opinions and views expressed or implied, in my profile [or on my page] are entirely personal and do not necessarily represent the opinions or views of any other person or organization, including the California Department of Public Health. The California Department of Public Health has not reviewed or approved, and is not responsible for, the material contained in this profile [or on this page].

- The Department's name, program names, telephone numbers, E-mail addresses, and images are not to be posted on social network profiles for employees for personal purposes. However, an employee may use his or her Department title for identification purposes. If the use of the title might imply endorsement, support or opposition of the Department with regard to any personal statements, including opinions or views on any issue, an explicit disclaimer must appear proximate to the material. See disclaimer above.

Appendix E: Sample CDPH Warning Banner

WARNING: This is a CDPH computer system that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Confidential, sensitive, or personal information contained in this system may not be accessed, used, disclosed or transmitted unless you are authorized to do so and unless you act in accordance with any limitations imposed on your access or use of this information. Unauthorized or improper use of this system or of any information contained in this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. **LOG OFF IMMEDIATELY**, if you are not an authorized user or you do not agree to the conditions stated in this warning.