CHAPTER 4

ARTICLE 45-INFORMATION SECURITY

Revised – December 5, 2003

49020.1 Policy

It is the policy of the California Department of Corrections (CDC) to protect against the unauthorized modification, deletion, or disclosure of information included in agency files and databases. The Department regards its information assets, including data processing capabilities and automated files, to be essential resources. The Department shall assume full responsibility for ensuring the security and integrity of its automated information.

49020.2 Purpose

The purpose of this policy is to establish and maintain a standard of due care to prevent misuse or loss of Department information assets. This policy establishes internal policies and procedures that:

- Establish and maintain management and staff accountability for the protection of departmental information assets.
- Establish and maintain processes for the analysis of risks associated with departmental information assets.
- Establish and maintain cost-effective risk management processes intended to preserve the Department's ability to meet program objectives in the event of the unavailability, loss, or misuse of information assets.
- Protect departmental employees who are authorized to access the Department's information assets from temptation, coercion, and threat.

49020.3 Statutory References Concerning the Confidentiality and Security of Information Within CDC

State Administrative Manual (SAM), § 4841 requires the director of each State department that uses, receives, or provides information processing services to designate an Information Security Officer (ISO) who shall be responsible for implementing State policies and standards regarding the confidentiality and security of information within the Department. These policies and standards shall include, but are not limited to, strict controls to prevent unauthorized access of data maintained in computer files, program documentation, data processing systems, data files, and data processing equipment located physically in the Department. and dissemination of information under the control of California State agencies is found in the State Constitution, in statutes, and in administrative policies:

- Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.
- The Information Practices Act of 1977 (Civil Code, § 1798, et seq.), places specific requirements on State agencies in the collection, use, maintenance, and dissemination of information relating to individuals.
- The California Public Records Act [Government Code (GC), §§ 6250-6265], provides for the inspection of public records.
- The State Records Management Act (GC, §§ 14740-14770) provides for the application of management methods to create, use, maintain, retain, preserve, and dispose of State records, including the determination of records essential to the continuation of State government in the event of a major disaster. SAM, §§ 1601-1699 contains administrative policies to implement provisions of this law.
- The California Penal Code (PC), § 502 covers the following offenses:
  - Manipulating data, a computer system, or computer network to devise or execute a fraud.
  - Knowingly accessing and without permission taking copies or using any data from a computer or taking any supporting documentation, internal or external, to a computer.
  - Theft of computer services.
  - Knowingly accessing and without permission damaging data, computer software, or computer programs, internal or external, to a computer.
  - Disrupting or denying computer services to an authorized user.

The Federal Copyright Act of 1976 provides for the prosecution of persons guilty of the theft of computer programs.

49020.4 Departmental Approach to Information Security

The departmental approach to information security consists of the following components:

- Policies to ensure that information security and information privacy are incorporated at each phase of the information systems development life cycle.
- Conduct periodic risk assessments in accordance with SAM, § 4842.1 to ascertain the threats and vulnerabilities that impact CDC's information assets, and implement appropriate mitigations.
- Provide information security training to all employees who use information assets in the course of their assigned duties to ensure awareness and understanding of the Department's policies.
- Conduct information security audits for compliance with security policies. Report deficiencies or noncompliance with CDC security policies to management for corrective action.
- Adherence to requirements established in SAM, § 4841.
- Periodically review security policies for changes that may be necessary as a result of technology evolution or changes in department operations.

49020.5 Information Security Definitions

The following terms are defined for purposes of this article:

Access

To gain entry into, or to instruct or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

Authorization

The granting of permission to execute a set of operations in a system.

Access Control

Tasks performed by hardware, software, and administrative controls to monitor a system's operation, ensure data integrity, perform user identification, record system access and changes, and grant access to users.

Accountability

The ability to trace violations or attempted violations of system security to the individual(s) responsible.

Access Management Group

A group that is responsible for access permissions granted to CDC's Information Assets, including the CDC Network, and departmental applications and databases.

Authentication

The procedure for identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

Baseline Security Controls

A set of general controls designed to meet an acknowledged level of security control that should be in place within all properly run computer centers.

Bulletin Board System

An electronic message system that runs a computer and allows users to enter and read information.

CDC Network

The system of telecommunication devices, workstations, servers, and peripherals used to provide inter- and intra-facility connectivity that enable sharing of information assets and electronic communications between CDC employees. The CDC Network is managed by Information Systems Division (ISD).

Call Back

A method used to identify a terminal or modem that is dialing into a system, whereby the system disconnects the calling terminal or modem and then reestablishes the connection by dialing the telephone number of the calling terminal or modem.

Classification

The assignment of information, including a document, to a category on the basis of its sensitivity concerning disclosure, modification, or destruction.

Computer-Based Tools

Software or computer programs that improve or enable a user's ability to configure and manage information technology components.

Computer Contaminants

Any set of computer instructions that, outside the intent and without the permission of the owner of such information, is designed to modify, damage, or destroy a computer, system, or network, or to record or transmit information within a computer, system, or network. Such contaminants include, but are not limited to, the group of self-replicating or self-propagating computer instructions commonly termed viruses, trojans, and worms, which are designed to affect computer programs or data, consume computer resources, modify, destroy, record, or transmit data, or otherwise usurp the normal operation of the computer, computer system, or computer network.

Computer Network

Any system that provides communication among one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

Computer Program or Software

A set of instructions or statements or related data, that when executed in actual or modified form causes a computer, computer system, or computer network to perform specified functions.

Computer Security

The technological safeguards and managerial procedures that can be applied to computer hardware, programs, data, and facilities to ensure the availability, integrity, and confidentiality of computer-based resources. This can also include assurance that intended functions are performed as planned.

Computer Services

Includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, system, or network.

Computer System

A device or collection of devices, including support devices but excluding calculators that are not programmable and not capable of being used in conjunction with external files, one or more of which contains computer programs, electronic instructions, input data, and output data, and which performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

Confidential Information

Information maintained by State agencies that is exempt from disclosure under provisions of the California Public Records Act (GC §§ 6250-6265) or other applicable State or federal laws.

Critical Application

An application so important to the Department that its loss or unavailability 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 Department employees, the fiscal or legal integrity of departmental operations, or the continuation of essential programs. All CDC departmentwide information systems are critical applications.

Custodian of Information

An employee or organizational unit (such as a data center or information processing facility) acting as caretaker of an automated file or database.

Data

A representation of information, knowledge, facts, concepts, computer software, computer programs, or instruction. Data may be in any form, such as in storage media, as stored in the memory of the computer, in transit, or as presented on a display device.

Decentralized Applications

Systems that run on more than one computer in geographically separated locations. The term also refers to systems that are not supported by a single organization, such as ISD.

Denial of Service

A situation where authorized access to information assets is prohibited because unauthorized usage has consumed all available resources. A "Denial of Service" attack is often caused by computer contaminants such as viruses and worms.

Documentation

Information about how specific applications are constructed, maintained, and used. It includes, but is not limited to, system and program design specifications, record formats, report layouts, program source and object code, job control language specifications, run instructions, key entry instructions, and data definitions.

Distributed Data Processing System

A CDC department information system. [Department Operations Manual (DOM), Chapter 4, Article 40, Distributed Data Processing System].

E-mail

Written communication transmitted electronically using computers connected to network(s).

Handheld Computer

Synonym for Personal Digital Assistant.

Information Assets

Any documents, electronic files, or records that contains or is used to process, manage, or store information necessary to the operation of CDC.

Information Technology

All hardware and software used to collect, store, manage, and transfer information.

Information Integrity

The condition in which information or programs are preserved for their intended purpose, including the accuracy and completeness of information systems and the data maintenance within those systems.

Information Security

The protection of automated information against unauthorized access (accidental or intentional), modification, destruction, or disclosure.

Information Security Architecture (ISA)

Compilation of the strategy, guidelines, and standards comprising CDC's program to ensure the protection and security of information assets.

Injury

Any alteration, deletion, damages, or destruction of a system, network, computer program, or data caused by unauthorized access.

Internet

The World Wide Web (WWW), consisting of a network of networks.

Intranet

A term that refers to a closed network of networks. In the context of CDC, it refers to the whole of the information assets that comprise the CDC Network.

Local Area Network

A Local Area Network (LAN) is a computer network consisting of telecommunications devices such as routers, hubs, switches and firewalls, and computers such as workstations, servers, and peripheral devices.

Mainframe

Referring to large computers typically housed in a data center environment, and running legacy systems. Mainframe computers have security components (such as Resource Access Management System) integrated into the operating system, and can support many hundreds of simultaneous users.

Malicious Code

Synonym for computer contaminant.

Midrange computer

Synonym for minicomputer.

Minicomputer

A class of computers upon which applications in the 1980's were implemented that are smaller in physical dimensions than mainframes, and require less overhead to maintain. Minicomputers use terminal access and support a few hundred simultaneous users.

Owner of Information

An individual in a particular position or an organizational unit having responsibility for making classification and control decisions regarding automated files or databases.

Parole-LEADS

A departmental application used to provide parolee information to local law enforcement agencies.

PC Coordinator

An individual who supports a group of users and the information assets accessed by that group of users.

Personal Digital Assistant (PDA)

Palm-sized computer that can sync with a workstation and allow user to refer to information from the workstation without having to print it out. Schedules, e-mail, documents and spreadsheets as well as reference material such as dictionaries and phone lists can be stored and accessed as needed. PDAs often are capable of wireless connectivity with LANs and the Internet.

Physical Security

The protection of information processing equipment against damage, destruction, theft, or unauthorized entry, and of personnel from potentially harmful situations.

Privacy

The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Production Application

A computer-based process that stores, manipulates, or reports departmental information.

Public Information

Any information prepared, owned, used, or retained by a State agency and not exempted specifically from disclosure requirements under the California Public Records Act, GC, §§ 6250-6265, or other applicable State or federal laws.

Resource Access Management Facility.

An application within IBM-based computer systems that reviews logons, passwords, and permissions before permitting access to information.

Risk

In the context of information systems, the likelihood or probability that a loss of information assets or breach of security will occur.

Risk Management

The process of taking actions to avoid risk or to reduce risk to acceptable levels.

Sensitive Information

Information maintained by State agencies that requires special precautions to protect it from unauthorized modification or deletion (See SAM, § 4841.3). Sensitive information may be either public or confidential.

Supporting Documentation

Includes, but is not limited to, all information in any form pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software that is not available generally to the public and is necessary for the operation of a computer, computer site, computer network, computer program, or computer software.

Teleprocessing Equipment

Computers, network components, and other devices that facilitate, enable, or depend upon data communications. Network devices such as, but not limited to, routers, hubs, wires, computers, and servers are teleprocessing equipment.

User Identification (ID)

The logon name an individual uses to access a computer or network system.

User of Information

An individual having specific limited authority from the owner of information to view, change, add to, disseminate, or delete such information.

Victim Expenditure

Any expenditure reasonably and necessarily incurred by the owner or lessee to verify whether a system, network, data, or computer program was altered, deleted, damaged, or destroyed by the access.

Virus

A computer contaminant. Viruses are often transmitted through e-mail.

Wide Area Network (WAN)

Two or more LANs connected together.

Wireless

Referring to communications transmitted without wires, such as radio, microwave, or infrared.

Workstation

Any device commonly called a microcomputer, PC, or terminal used for processing, storing, or sending information.

Worm

A computer contaminant. Worms are often introduced into a LAN or WAN through e-mail and then propagate themselves to other workstations on the network.

WWW

An abbreviation for World Wide Web. See Internet.

49020.6 Responsibility

The Department has established the necessary policies, procedures, practices, and controls to protect information assets from accidental or intentional disclosure, destruction or modification, and to comply with all applicable State and federal privacy legislation. Information assets covered by this article include, but are not limited to:

- All categories of automated information including, but not limited to, records, files and data bases.
- Information technology facilities, software, and equipment (including personal computer systems) owned or leased by CDC.

The following is a description of the organizational responsibilities for administering this program:

Director

The Director is responsible for establishing and maintaining an information security program within the Department. It is the responsibility of the Director to assure that information assets are protected from the effects of damage and destruction, as well as from unauthorized or accidental modification, access, or disclosure. Specifically, the Director is responsible for ensuring:

- Enforcement of State level security policies.
- Establishment and maintenance of internal policies and procedures that provide for the security of information technology facilities, software and equipment, and the integrity and security of the agency's automated information.
- Department compliance with reporting requirements related to security issues.
- Appointment of a qualified ISO.
- Participation of management during the planning, development, modification, and implementation of security policies and procedures.

ISO

SAM, § 4841 requires that each agency designate an ISO. Additionally, to avoid conflicts of interest, the following restrictions shall apply to the ISO:

- The ISO shall not have direct responsibility for information processing.
- The ISO shall not have direct responsibility for access management functions.
- The ISO shall not have direct responsibility for any departmental computer-based systems, or have a reporting relationship to an organization that has such responsibility.
- The ISO shall not have any special allegiance or bias toward a particular program or organization.

The ISO is responsible for overseeing Department policies and procedures designed to protect its information assets. In accordance with State policy, the ISO shall be accountable to the Director with respect to these responsibilities.

The responsibilities of an ISO include overseeing the following:

- Implementation of necessary procedures to ensure the establishment and maintenance of a security program.
- Establishment of security policies and procedures designed to protect information assets.
- Identification of confidential and sensitive information and critical applications.
- Identification of vulnerabilities that may cause inappropriate or accidental access, destruction or disclosure of information, and establishment of security controls necessary to eliminate or minimize their potential effects.
- Establishment of procedures necessary to monitor and ensure the compliance of established security and risk management policies and procedures.
- Coordination with internal auditors to define their role in automated information system planning, development, implementation, operations, and modifications relative to security.
- Coordination with the applicable data center's ISO or staff on matters related to the planning, development, implementation, or modification of information security policies and procedures that affect the Department.
- Acquisition of appropriate security equipment and software.
- Establishment of procedures to comply with control agency reporting requirements.
- Development and maintenance of controls and safeguards to control user access to information.
- Establishment of mechanisms to assure that Department staff (with particular emphasis on the owners, users, and custodians of information) are educated and aware of their roles and responsibilities relative to information security.
- Establishment of training programs for Department employees related to information security.

Technical Management

Department technical management has the following responsibilities relative to the Department's information security program:

- Ensuring that management, the ISO, assigned owners, custodians, and users are provided the necessary technical support services with which to define and select cost effective security controls, policies, and procedures.
- Ensuring the implementation of security controls and procedures as defined by the owners of information.
- Ensuring the implementation of system controls necessary to identify actual or attempted violations of security policies or procedures.
- Ensuring that the owners of information and the ISO are notified of any actual or attempted violations of security policies and procedures.

Program Management

Department program managers have the following responsibilities in relation to the Department's security program:

- Establishing the procedures necessary to comply with State information security policy in relation to ownership, user and, if appropriate, custodian responsibilities.
- Ensuring that State program policies and requirements are identified relative to security requirements.
- Ensuring the proper classification of automated information for which the program is assigned ownership responsibility.
- Ensuring the participation of the ISO and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and to protect information assets.
- Ensuring that appropriate security requirements for user access to automated information are defined for files or data bases for which the program is assigned ownership responsibility.
- Ensuring the proper planning, development, and establishment of security policies and procedures for files or data bases for which the program has ownership responsibility, and for physical devices assigned to and located in the program area(s). Ensuring that custodians of program information are provided the appropriate direction to implement the security controls and procedures that have been defined.
- Ensuring that procedures are established to comply with control agency reporting requirements.

Program Personnel and Users

Program personnel have the following security responsibilities:

- Implementing and monitoring data quality assurance functions to ensure the integrity of data for which the program is assigned ownership responsibility.
- Complying with applicable federal, State, and Department security policies and procedures.
- Complying with applicable federal and State statutes.
- Identifying security vulnerabilities and informing program management and the ISO of those vulnerabilities.
- Ensuring that management, the ISO, and assigned owners and custodians and other users are provided the necessary technical support services with which to define and select cost-effective security controls, policies, and procedures.
- Ensuring the implementation of security controls and procedures as defined by the owners of information.
- Ensuring the implementation of system controls necessary to identify actual or attempted violations of security policies or procedures.
- Ensuring that the owners of information and the ISO are notified of any actual or attempted violations of security policies and procedures.

Internal Auditors

The Information Security Unit of the Policy and Evaluation Division has the following audit responsibilities in relation to the Department's information security program (DOM, Chapter 4, Article 48, Electronic Data Processing Auditing).

- Examination of the Department's information security policies and procedures for compliance with State information security policies, including control agency audit requirements.
- Identification of possible corrective actions.
- Informing management, the ISO, and the owners, custodians, and users of information of audit findings.

Access Management

Access Management within CDC is:

- A critical responsibility of information system owners and custodians.
- An organizational unit within ISD.

The access management group and each organization with owner or custodial responsibilities for an information system have the following access management responsibilities:

- <u>Access Authorization.</u> The granting of permission to execute a set of operations in the system. At the lowest level, for example, this would be to grant permission for inmate trust personnel to access the classification of inmates on the Distributed Data Processing System (DDPS). At the highest level, for example, this would be working with the information system owners to physically allow access to a specific information system.
- <u>Access Control.</u> Enabling the performance of tasks by hardware, software, and administrative controls that would have the effect of monitoring a system's operation, ensuring data integrity, performing user identification, recording system access and charges, and granting access to users.
- <u>Accountability.</u> The work necessary to set up the ability to trace violations or attempted violations of system security to the individual(s) responsible.
- Additionally, the access management group of ISD shall maintain the central file of all signed self/joint certification statements and security agreements, and shall provide the ISO, management, and owners with appropriate status reports.

Information Security Coordinators

Every organizational entity that uses computer systems, or uses computer applications that are not directly supported by ISD shall designate an Information Security Coordinator (ISC) for each site maintained by that entity. The designated Security Coordinator shall be responsible for ensuring that applicable CDC policies and procedures are followed, and shall act as the security liaison to the ISO.

A procedure shall be developed by each of these organizational entities, subject to approval by the ISO. The procedure shall be constrained as follows:

- The designation of an ISC for the decentralized or control entity shall be in writing and shall identify the name, work address, and telephone number of the ISC.
- The access management group shall maintain a file of all current and past designated ISCs.
- The designated ISC shall be aware that they are the designated Security Coordinator and the responsibility that the designation entails.
- The designated ISC shall ensure compliance with information security policies and procedures, and with any security guidelines issued by the owners of decentralized automated systems.

Information Owners

The owners of information are responsible for classifying the information, defining precautions for its integrity, disposing of the information, defining initial levels of access need, filing security incident reports, securing signed security agreements and forwarding them to the Access Management Group, and identifying for the ISO the level of acceptable risk.

Each information system has one or more owners that are identified as part of the approval process for system development. Information owners must approve all major changes to information systems.

Information Custodians

The custodians of information, including the Teale Data Center, are responsible for complying with applicable laws and policies and procedures established by the owner and the ISO, advising the owner and the ISO of any threats to the information, and notifying the owners and the ISO of any violations of security policies, practices, and procedures.

49020.7 Reportable Incident Criteria

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. The following incidents shall be reported through the local ISC and chain of command to the Chief Deputy Directors and to the departmental ISO within three days of becoming aware that an incident has occurred:

- Unauthorized access to, or modification of, State-owned or State-managed data, including nonelectronic data such as reports, documentation, and hard copy files.
- Unauthorized use of, or access to, State computer resources, including computer networks and services, as well as systems not necessarily connected to a network.
- Unauthorized access to, or modification of, computer software, including operating systems, networks, configurations and applications. This includes the introduction of malicious software such as viruses, worms, and other malicious software.
- Deliberate or unauthorized acts resulting in disruption of State computer services, including "Denial of Service" attacks.
- Unauthorized use of user account or Internet domain names.
- Destruction of, or damage to, State information processing facilities.
- Break-in or other unauthorized access to State facilities resulting in compromise to the data or computer systems housed within those facilities.

CDC management shall investigate all incidents.

49020.7.1 Incident Report Format

The following information concerning each incident shall be reported to the ISO within three working days of becoming aware of the occurrence of the incident:

- Date and time.
- Location.
- Description of what happened.
- Estimated damages.
- Description of corrective action, taken or planned.
- Estimated costs associated with corrective actions.
- If known, identity those responsible for the incident.
- Descriptions of actions taken or planned against those responsible for the incident.
- Contact name and phone number.

The report submitted to the ISO shall be signed by the appropriate Warden, Regional Parole Administrator, Deputy Director, or Assistant Director. Incident reports shall be forwarded to the Department of Finance (DOF) within five business days of the initial report, and shall be signed by the ISO and the CDC Director. The Highway Patrol shall be notified of the occurrence of an incident within one day of receipt of the initial report.

49020.7.2 Consequences of Information Security Violations

During the time that a suspected violation is under investigation, the suspected violator's access privileges may be revoked or other appropriate action taken to prevent harm to CDC.

All violations of security policies or procedures are subject to disciplinary action. The specific disciplinary action that shall be taken depends upon the nature of the violation and the impact of the violation on CDC's information assets and related facilities. A partial list of potential disciplinary actions follows:

- Written reprimand.
- Suspension without pay.
- Reduction in pay.
- Demotion.
- Dismissal.
- Criminal prosecution (misdemeanor or felony, State or federal).

49020.7.3 Failure to Correct Information Security Deficiencies

Should any audit indicate that the State's security policies are not established or that the Department has not taken corrective action with respect to security deficiencies, the Department may be subject to any or all of the following:

- Further audit and review by the Financial Performance Accountability Unit of the DOF.
- Revocation by the DOF of delegated approval authority for information technology projects.
- Application of penalties specified in GC, § 1222.

49020.8 Information Security Ownership/Authority

An owner of CDC information must approve all requests for access to such information under his or her control. Approval authority may be delegated to a designated representative. The owner has an obligation to restrict access to the specific information to instances that are necessary and sufficient to meet the demonstrated need or right of the requestor. The owner shall consult with ISD to determine the most appropriate on-line access mechanisms for a specific request, keeping in mind that ISD is obligated to restrict the mechanisms to those that are necessary and sufficient to meet the requestor's need for, or right to, such information.

The owner is ultimately responsible for the integrity of the entrusted information. This responsibility requires that the owner have control over who can access, modify, disclose, or destroy information. The owner shall exercise the responsibility to communicate information security requirements to all appropriate personnel, and to make use of all available security features. Additionally, the owner shall determine that implemented security measures are adequate to meet the requirements of the application, and ensure that an employee's access authority is removed immediately upon separation or change of duties such that access is no longer necessary.

49020.9 Confidentiality of CDC Information Assets

For administrative purposes, all information residing on CDC's computers that is considered to be sensitive or confidential shall be treated as such by all persons who have access to it and shall be protected from unauthorized access.

No confidential information shall be present on any computer resource, including workstations, that is not under CDC's direct control unless authorized on a case-by-case basis by the ISO and the owner of the information.

Appropriate procedures to utilize confidential CDC information on any of CDC's computer resources, including any computer such as mainframes, mid-range, workstation, and other information assets on the CDC network are outlined in this article. The level of security measures shall be commensurate with the classification of the information involved.

49020.9.1 Confidentiality of Security Mechanisms

The specific security mechanisms used by the Department to control access to its information resources are confidential.

Information concerning specific details of access controls shall not be divulged except on a need-to-know basis, and only then to persons for whom there are signed security agreements on file.

49020.9.2 Confidentiality of Production Application Software

All documentation concerning production applications residing on CDC's mainframes, midrange, and workstations is confidential.

Appropriate procedures to protect and preserve the confidentiality of applications documentation are to be developed by each division that has responsibility for, or custody of, such documentation. The procedures shall ensure that documentation is not divulged except on a need-to-know basis, and only then to persons for whom there are signed security agreements on file.

49020.9.3 Confidentiality of Information on CDC Information Systems

Appropriate procedures shall be developed by each CDC Division to protect and preserve the confidentiality of the Department's information stored or residing in or on CDC controlled environments, such as the CDC Network, individual stand-alone desktop and laptop workstations, browser-based applications such as Parole-LEADS, and the DDPS. Additionally, no confidential information shall be faxed, reproduced (e.g., photocopied), distributed via e-mail, downloaded to a nonconfidential system, given to an unauthorized recipient, or transmitted by telephone to any entity without appropriate security controls in place that are documented in the CDC ISA.

49020.10 Access to Information Assets

Access to any CDC computerized information on any CDC computers or the Teale Data Center is restricted to authorize persons. Any person requiring such access shall:

- Be a State employee or a bona fide representative of the Department.
- Demonstrate either a need for, or a legal right to, the information.
- Receive formal authorization from the owner of the information.
- Accept legal responsibility for preserving the security of the information.

The sensitivity of the information residing in CDC's computerized environments requires strict controls over who is allowed access to that environment, which information may be accessed, and how that information may be accessed.

The following uniform access authorization procedure assumes that all pertinent procedures have been followed, and all CDC-required system approvals have been obtained. This procedure is for access to existing information resources.

The uniform access authorization procedure is as follows:

- The requestor shall complete a risk analysis. The risk analysis shall address all threats created by the additional access requirements and the necessary controls.
- All access requests, including the risk analysis, shall be sent to the system owner with a copy to the ISO. The request shall contain the following:
    - The name of the requester.
    - The specific information for which access is desired.
    - The reason(s) why the requestor has a need for, or right to, the information.
    - The frequency and duration of the requested access.
    - The type of access (e.g., read, update, copy, etc.).
    - An approval signature block for the owner's approval.

After the owner approves the request for access and returns it to the requestor, the approval is then routed to either ISD or the requesting organization's ISC for action.

49020.10.1 Annual Information Security Self-Certification

All CDC employees requiring access to CDC information assets are responsible for annually self-certifying that they are in compliance with applicable CDC information security policies. The ISO is responsible for ensuring compliance with this policy. Responsibility for the dissemination of the policies rests with the owner and the designated security coordinator; responsibility for compliance rests with the end-users.

Appropriate decentralized and control entity procedures shall be developed by each CDC unit that owns or has custody of decentralized applications including, but not limited to, the applications delineated in DOM, Chapter 4, Article 31, Personal Computer Systems, CDC Network access, use of stand-alone computers to complete CDC work, and access to the Internet. Each such procedure is subject to approval and audit by the ISO. The procedures are constrained by the following:

- A separate statement of self-certification shall be signed by every employee that access or uses CDC’s information assetts.
- Each self-certification shall be signed by a representative of the senior management of the organizational entity.
- Each self-certification is to be filed with the local ISC, and available for review by the ISO.

49020.10.2 Information Security-Responsibilities of Password Owners

Access to CDC's information systems is restricted by password to only authorized persons. Authorized persons shall never reveal their passwords to anyone for any reason. Authorized persons using a computer shall log off or activate a password-protected screensaver before leaving the immediate vicinity of the computer or terminal. Additionally, no ability shall exist for a user to store, load, or invoke the log on process on any CDC computer, by any method that includes the user Resource Access Control Facility (RACF), ID or the password. Violation of this policy may result in the revocation of all access privileges and appropriate disciplinary action. Such disciplinary action may be based not only on the violation itself, but also on all activity performed by those obtaining access to a system or information asset due to a violation of this policy.

The password is a major "key" to the integrity of CDC's automated environment. The password policy exists to protect the integrity of that “key.”

User IDs shall never be shared. User ID security is backed up by the existence of passwords. Owners are responsible for anything for which their password is used. Therefore, as a matter of self-protection, the password owner shall:

- Not tell anyone what the password is.
- Not write down the password.
- Not use an obvious password. Obvious passwords include one's name or nickname, the names of one's children, one's user ID, names or words associated with hobbies ("DANCER," "SKIER," “GOLFER,” etc.), names associated with favorite books, TV shows or movies ("JEDI," "FRODO," "PICARD", "RHETT," etc.), "SECRET," "SECURE," "PASSWORD," all spaces or the “enter” key, “9999999”, “XXXXXXX,” driver's

license, social security numbers, the name of the current month, etc.

- Not use words that can be looked up in any dictionary, including foreign languages (e.g., Latin).
- Use non-obvious passwords, such as word combinations rather than single words ("COMPUTERUSER," "SKIBUM," "IAMADANCER," etc.) intentionally misspelled words ("KRAKER," "KORECTUNS," etc.), or random combinations of letters and numbers, etc.
- Use passwords that are at least seven characters long.
- Change the password in accordance with specific application requirements, every 30 to 90 days, depending on the application.

If the password owner becomes aware that a correct password is being rejected, that user should immediately notify the local ISC and the ISO, since this may indicate that someone has discovered the password and has changed it without the owner's permission, resulting in the owner no longer knowing his or her own password.

If a password is forgotten, the local ISC or the CDC Help Desk shall be contacted. They shall validate the owner's identity and give a new temporary, one-time password. The owner shall change this password immediately.

If anyone asks for a password, the owner shall refuse to provide it and shall refer the person to a supervisor. The owner shall then notify the supervisor.

Anyone who knows that any password has been compromised should take the following actions:

- Notify the ISC.
- Notify the ISO.
- Complete a "security incident report."

49020.10.3 Information Security-Responsibility of Supervisors

People are provided passwords because their jobs require them to access CDC information systems. When a password owner terminates employment or is reassigned to duties that do not require such access, the immediate supervisor shall, without delay, notify the applicable party of the change.

The authority to access CDC computers entails a significant risk to the Department's ability to function. Such authority is restricted to persons with a demonstrated need for access. Because that need is, by definition, a function of the person's specific job duties, any change in those duties requires a reevaluation of the need for access. If the duties change such that the need for access no longer exists, the access shall be revoked.

If any password owner changes job duties (via resignation, promotion, transfer, reorganization, separation, etc.), that individual's immediate supervisor shall initiate the following:

- Reevaluate whether the person's new duties still require the authority to access CDC's computers.
- Notify the local security coordinator or the access management group if the person no longer requires access authority.
- Notify the owner of the relevant CDC information so that the appropriate paperwork can be initiated to document the removal of the person's access privileges if the person no longer requires access authority.

The lack of use of the access authority is assumed to be proof that the authority is no longer required. Access authority to information assets may be revoked without notice if they are not used regularly.

49020.10.4 Requesting Authority to Access CDC's Mainframe Environments

Access to an entire mainframe environment shall not be authorized. Access to specific portions of that environment, such as but not limited to the system development facilities, shall be authorized for specific organizations. Access to a specific application can be authorized by the Information Owner as a means of meeting a specific request for specific information.

49020.10.5 Unattended Workstations

Active workstations or terminal sessions must not be left unattended. Any authorized or unauthorized activity on an unattended workstation will be attributed to the person whose logon and password activated the terminal or workstation. All sessions shall either be terminated when leaving the immediate area, or protected with a password-activated screensaver.

49020.11 Restrictions on Using CDC Information Assets

The use of all CDC information assets including any mainframe computers, minicomputers, notebook, laptop and workstation desktop systems, network components, and applications run on or accessed from CDC computers is restricted to official CDC business.

49020.12 Information Systems Access Control

All access to CDC's information systems shall be protected by at least user ID/password access control. CDC's mainframe computers shall operate within the constraints of RACF. Any software installed on mainframe computers that uses its owner password protection features shall provide for nondisplay of and, restricted control over, passwords.

Because RACF is the facility used to logically protect the resources on CDC's mainframe computers, no software that allows RACF to be bypassed or compromised may be installed on those computers.

49020.13 Segregation of Duties in the Information Security Program

There shall be a strict separation of duties between, and within, all organizations responsible for using, operating, and developing computer-based information systems. Separation of duties shall be maintained to ensure a separation of responsibilities for initiating and authorizing transactions, recording of transactions, and custody of assets. Segregation of duties, similar to that required in manual systems, shall be implemented in computerized systems.

The following guidelines shall be used regarding such separation of duties:

- Convert and conceal - No one person should be able to convert a resource to their personal use and be able to conceal the action.
- Custody and control - No one person should have custody of an asset and at the same time be solely responsible for the accounting for that asset.
- Custody and access - No one person shall have custody of an asset and, at the same time, have unrestricted access to the records pertaining to that asset.
- Origination and authorization - No one person shall both originate and authorize a transaction.
- Originate and maintain - No one person shall both enter a transaction and maintain the related master file.
- Access and restriction - Access to transactions shall be on a need-to-know basis.

ISD is charged with the responsibility for the development and maintenance of computer-based systems for CDC. In this capacity, ISD provides a service to actual or potential users of computer-based information systems. In addition, there are several computer "users" groups throughout the Department. Each of these organizations is providing a service to all actual or potential users of computer-based information systems.

To ensure that assigned responsibilities are met and that separation of duties is maintained, individuals/programs shall not originate or authorize transactions, have custody or control over online data processing assets, or have the authority to originate master file changes. Source documents shall originate and be controlled by functions independent of such persons/programs.

Appropriate procedures shall be developed by ISD, subject to approval by the ISO, to ensure that adequate controls exist to ensure the separation of duties and responsibilities.

The procedures may include variances to the Change Management Process in order to resolve failures of critical applications. Such variances shall provide for audit trails and retroactive release or approval documentation, and require the prior approval of the ISO.

49020.14 Information Security Awareness

It is the responsibility of CDC management at all levels to ensure that personnel are aware of their responsibilities:

- All employees are accountable for the implementation of information security policies and procedures within their areas of responsibility.
- Accountability requires that employees be aware of the Department's information security policies and procedures.
- All employees that are owners, users, or custodians of a departmental information system shall receive annual information security training.
- Security awareness training shall be given as a part of each employee's orientation and annually thereafter. Each employee shall receive a copy of the security policy. All employees that access or use information assets shall annually complete and sign a self-certification form.
- All employees changing jobs, or exiting owner, user or custodian status, shall have their security privileges revoked immediately, and such persons shall be prevented from having any further opportunity to access information.
- Employees with the status of owner, user, or custodian shall have a job descriptions that details that status and the security requirements therein.
- Systems, including CDC's mission critical systems and Internet access, shall be monitored and activity logs maintained as per the Department's ISA.

49020.14.1 Security Awareness Training Within CDC

All persons who have access to any CDC information shall be provided security awareness training at the time such access begins, and at least annually thereafter. The ISO shall ensure that security awareness training is provided prior to the employees' self-certification of their awareness of CDC's information security policies, and the renewal of access privileges to CDC information assets.

Security awareness training falls into the following two categories:

Information Security

All individuals having access to CDC information shall be made aware of the background, scope, and objectives of CDC's information security program and of specific CDC information security policies and procedures that are applicable to the level and type of access granted to the individual. The minimum training shall consist of completion of the departmental computer-based training module.

Incident Reporting

All CDC employees shall also be made aware of the events and activities that constitute threats to the organization for which they work, and of the actions to be taken when confronted by those events or activities.

49020.15 Physical Access Control to Information Assets

The sensitivity of CDC's information assets and personnel safety requires that all CDC computer facilities have physical controls to prevent unauthorized access.

Each owner and custodian of departmental information systems shall establish physical controls over their information assets. This requirement applies to workstations with confidential or sensitive information and includes network and data communications components, as well as application and database servers.

49020.16 Confidential or Sensitive Information Stored on Workstations

The nature of information classified as confidential or sensitive requires strict controls over access to such assets (SAM, § 4989.7).

Confidential or sensitive information may be stored on or accessed with workstations in accordance with the following provisions.

- Only authorized personnel may have access to confidential or sensitive data.
- Workstations containing or capable of accessing such data shall be equipped with hardware and/or software that provide for authentication techniques, such as password protection of confidential files.
- Confidential and sensitive files shall be encrypted, if the owner deems it necessary. Encryption software must comply with standards documented in the ISA.
- Backup files of confidential data shall be maintained in a locked cabinet away from the location of the workstation containing the program providing access to such files.
- Security hardware/software shall comply with standards documented in the ISA.
- At least two individuals shall be authorized access, and have knowledge of, the location where data files, backup files, and forms are stored.

49020.16.1 Software Controls on CDC's Workstations

The following software controls shall be established for all CDC workstations:

- No software shall be loaded, installed and/or activated on any CDC workstation without prior review and written approval from the local ISC and the requestor's supervisor, or ISD.
- Controls that ensure that CDC is in compliance with all State-mandated requirements (SAM, §§ 4820, 4989.7, and 4990.1).
- Appropriate procedures shall be developed by ISCs for use by each CDC division that has workstations. These procedures are subject to approval by the Department's ISO, and are constrained by the requirements of the CDC workstation policy.

49020.16.2 Data File Transfers

Electronic transfer (file transfer) of information to or from any CDC information system file or database is restricted to authorized persons who shall use an approved file transfer mechanism. The same level of protection afforded the information in its originating system shall be provided by the computer environment to which the information is transferred.

Transfer of information from one CDC computer to another does not alter the sensitive nature of the information or eliminate the need to protect the confidentiality of the information. An appropriate procedure shall be developed by ISD for use by each CDC division that uses file transfer mechanisms. The procedure shall be constrained as follows:

- The user is responsible for providing the necessary controls to secure all confidential information maintained in the workstation environment. A Security Plan must be approved by the ISO prior to confidential or sensitive information being stored on a workstation.

- Dial-up access to the Department's databases is prohibited.
- All requests to transfer information shall be approved by the owners of the information and the custodians of the information. The owners shall provide the necessary authorization for access (if the request is approved), and the custodian shall provide the methodology.
- Confidentiality of information shall be maintained.
- Any workstation performing file transfers shall be subject to additional hardware and software controls (e.g., encryption and dynamic password user authentication) to enhance the security environment of the workstation.

Interagency data file transfers are subject to requirements described above as well as those defined in DOM, Chapter 4, Article 45, Information Security, § 49020.5.

49020.17 Information Security Architecture

Teleprocessing equipment in CDC's automated network environment (computers and peripherals) shall be secured against access by unauthorized persons. Any equipment that is not stand-alone is considered teleprocessing equipment. This includes all workstations that are connected to each other or to any other mainframe, mini or micro, whether by dial-up, cabling (including but not limited to coax, twisted pair, and fiber), LANs, Gateways, routers and all other network components. Access to CDC's network shall be restricted to CDC employees. The methods by which CDC's teleprocessing equipment is secured shall be documented in the CDC ISA. Any exception or modification to the ISA must be approved in writing by the ISO prior to implementation.

The ISA shall include descriptions of procedures to protect and preserve the teleprocessing equipment from access by unauthorized persons. The procedures are constrained by the following:

- Only authorized personnel shall have access to terminals, printers, control units, concentrators, telephone wiring panels, modems, and emulation cards.
- Control of access through the CDC telecommunications system to the Internet is the responsibility of the ISD, and is administered in accordance with the ISA. Additional access not described in the ISA constitutes a request for a modification to the ISA and must be submitted and approved in accordance with this policy prior to implementation.
- Persons not authorized to access the CDC's telecommunications system shall obtain approval from the designated local ISC. Unauthorized persons include representatives of control agencies, CDC personnel from another site, equipment vendors, telephone companies, etc.
- Any division with custodianship of decentralized applications shall locate equipment in restricted areas that shall be monitored during working hours and locked during unattended periods.
- Access to computers, either connected to a CDC network or stand-alone, shall be limited by the use of a password-protected screensaver and/or key-controlled access to the power supply and/or keyboard with the keys physically removed and stored away from the workstation.
- Computers connected in any way to CDC's telecommunications system or stand-alone computers with modems connected to them may not be located in areas where inmates have access, except when work assignments involve janitorial duties and the inmates are under the direct and constant supervision of custody staff.
- Control units shall be locked whenever possible and the keys removed and stored in a secure environment.
- Storage mediaincluding, but not limited to diskettes, CDs, removable hard drives and tapes, shall be removed from equipment that reads them and stored in a secure environment when not in use.
- Documentation pertaining to the hardware, system software, and configuration of the CDC's telecommunication system are confidential.
- All facility phone rooms and other locations where network components are kept shall be labeled "Out of Bounds. Authorized Personnel Only".

49020.17.1 Requests for Modifications of the Information Security Architecture

The sensitivity of CDC's automated information assets requires strict controls over who can use equipment that is configured to access these assets. Also, the monetary value of the equipment itself warrants physical controls to deter theft or damage to the equipment.

A risk analysis shall be carried out prior to any major change to the Department's data networking capabilities. This risk analysis must be conducted in accordance with DOM, Chapter 4, Article 46, Information Systems Risk Management, and submitted with a description of the proposed change and reasons for considering the change, for approval to the ISO prior to implementation of the proposed changes.

Changes in the physical location of telecommunications equipment and switching of terminals and computers from one control unit to another require approval of the network owner (in most cases the ISD).

The teleprocessing coordinator's staff shall conduct the actual activities.

49020.17.2 Modem Usage

The critical and sensitive nature of the informational resources residing in CDC's computers requires stringent controls of devices attached to these computers, and over which persons are allowed to use these devices.

All access to the CDC's systems shall be monitored and controlled by ISD. All other means of accessing CDC systems including, but not limited to, wireless communication devices and dialup modem, are prohibited unless approved by the ISO.

Modem use is restricted to computers not connected to the CDC Network, unless such use is an approved part of the ISA. Requests for additional modems to be used within the CDC teleprocessing environment are subject to approval.

Modems may be used to access remotely the CDC network resources through ISD-supported access mechanisms. They may also be used to provide access to the Internet and specific destinations, and e-mail capability, when such access is not available through the CDC network resources. Justification and procurement of modems for these purposes shall be conducted in accordance with DOM, Chapter 4, Article 41, Departmental Workgroup Computing Policy.

Specific restrictions on the use of modems are:

- There shall be no inmate or parolee access to any computer for which a modem has been approved. Computers that are attached to modems shall not be located in areas where inmates or parolees have access.
- No applications that were developed by inmates shall be implemented on a modem-equipped computer.
- No modems shall be installed on any computer that is a part of a LAN that has been approved for inmate use.
- The location and usage of all modems must be tracked and monitored at all times.
- Computers with "pocket" modems may not be used within the secured perimeter of facilities. They shall not be used in parole

offices unless the area where the modem is to be used is secured from parolee access.

- Non-CDC computers shall not access the CDC Network via modem.

49020.17.3 Documentation of Changes to CDC's Teleprocessing Environment

Any modification to the ISA must be accompanied by a risk analysis and must be approved by the ISO.

An appropriate telecommunications change log and logging procedure shall be used by the ISD to provide an audit trail of all approved changes to the ISA. At a minimum this log shall contain entries for the following:

- Alterations in the number, type or location of terminals, control units, modems, concentrators, phone lines, prots, protocol converters, front-end processors or communications controllers, encryption-decryption devices, dial-up ports, etc.
- Changes to the existing control software configuration, such as new additions, releases, modification, and version changes.
- Changes due to new applications.

Changes to on-line applications if those changes impact the vulnerability or integrity of the Department's teleprocessing environment.

49020.17.4 Installation of Changes to CDC's Teleprocessing Environment

Changes to the teleprocessing environment that require a modification to the ISA shall not be implemented without the documented approval of the ISO.

This section is intended to ensure the maintenance of adequate controls over the teleprocessing environment. The ISA policy provides a method for identifying the teleprocessing environment changes that have a security impact.

CDC's access management group is responsible for installing certain types of the teleprocessing environment changes into production. The ISO shall provide the access management group a copy of the notification form for each teleprocessing environmental change that:

- The access management group is responsible for installing into production.
- Is identified as having a security impact.

49020.17.5 Accessibility of Mainframe Systems

Access to mainframe systems software is restricted to ISD. Access to mainframe systems software for any other organization or individual is forbidden. Exceptions shall be granted only after a thorough review within ISD, and approval of the ISO. If it is essential that mainframe systems software access be provided, it shall be restricted to the specific commands, such as Clists, Procs, Panels, and Applications, that are necessary and sufficient to meet the informational needs of the specific organization or individual, and such access shall be restricted to the time frame appropriate to the user's needs.

The power of the tools available in mainframe systems constitutes such a risk to the security and integrity of CDC's sensitive information resources that their use shall be severely restricted.

All requests for temporary or short-term user IDs (e.g., user IDs for contract programmers) shall indicate that they are limited term requests and shall specify the estimated date on which the user ID shall no longer be needed.

Requests for access to environments other than that normally given shall include justification.

49020.17.6 Physical Security Controls

No unauthorized hardware (e.g., line monitors, modems, nodes, gateways, bridges, etc.) or unauthorized software (refer to approved list maintained by ISD) shall be loaded, installed, or activated on any system connected to the CDC Network. Any installation that requires a modification to the ISA must be approved by the ISO prior to implementation.

The installation of non-CDC teleprocessing equipment, including computers, network, and communications devices is prohibited without prior written approval from the ISO.

Implementation of non-CDC teleprocessing equipment must adhere to the same security policies governing CDC teleprocessing equipment, specifically, those policies regarding inmate access to computers and areas where computers are used.

Portable and handheld telecommunications devices such as pagers, cell phones, and palm-sized computers are not allowed in inmate-accessible areas without prior written approval of the ISO.

The purpose of this section is to provide controls to ensure that CDC is in compliance with all mandated guidelines (SAM, § 4989.7) and to protect accessible information residing on a LAN system.

49020.18 Inmate Use of Computers

It is the policy of the Department to allow inmates or parolees access to computers, computer terminals, or computer keyboards only within the constraints of the policies contained in this article.

Any request for exception shall be referred to the ISO for review.

49020.18.1 Restrictions on Computer-Knowledgeable Inmates

Inmates who have a history of computer fraud or abuse, as defined in Penal Code (PC), § 502, shall not be placed in any assignment that provides access to a computer.

Inmates that have documented histories of computer fraud or abuse, as noted during the initial classification process, shall be identified on the initial classification chrono. Any occurrence of computer abuse after admittance to the prison system shall also be recorded in the inmate's records.

Inmates who have knowledge of computer use, programming experience or other skills that exceed assigned staffs' ability to monitor their activity on computers may not access computers. Staff assigned to supervise inmates using computers shall be able to monitor inmates' activity.

49020.18.2 Inmate Access to Computer-Based Tools

Inmates shall not be allowed access to any computer-based tools that could be utilized to create a virus, trojan, worm or cause damage to data files or a computer's operating system, except in an approved Computer Refurbishment Program.

49020.18.3 Inmate Access to Computers and Telecommunications Devices

Inmates may access workstations for the purpose of completing specific tasks or assignments while under direct and constant supervision. The approved uses of workstations by inmates shall be carried out only under very tightly controlled circumstances:

- Each computer shall be labeled to indicate whether inmate access is authorized.
- Computers used by inmates shall not be used concurrently for any other purpose.
- The local ISC shall approve or disapprove the movement of computers from an "inmate use" status to other work and vice versa.
- Inmates with a work assignment involving a particular computer shall not be assigned to work on other computers.
- Areas where inmates are authorized to work on computers shall be posted as such.

- All inmates shall be under the supervision of a knowledgeable employee within a controlled, designated area when using computers.
- There shall be no communications capabilities in the designated area, such as a telephone line, computer network line, telephone punch panel, cell phones, wireless communication devices such as pagers or handheld computers, or radio communication devices.
- Inmates shall not have access to computer utility programs used to modify the functionality of the computer or to view system configuration information, except in an approved Computer Refurbishment Program.
- Inmates shall not have electronic storage media in their possession except within an approved area.
- Inmates may not have access to computer application development tools.
- An inventory and appropriate controls shall be maintained on all diskettes. Diskettes for inmate use shall be labeled "For Inmate Use." Reports and other printed output from inmate-utilized computers shall be reviewed closely by staff, and appropriate distribution of such output shall be monitored.
- Inmates shall not have access to the operating system of any computer. Inmates shall not have access to any interface that allows access to the system configuration of any computer including, but not limited to, dialogue boxes, setup, and configuration screens. Additionally, inmates shall not have access to operating system commands that allow viewing or modification of any aspect of a computer operating system or the configuration of a computer, except in an approved Computer Refurbishment Program.
- Inmates shall not be allowed to load software onto hard disks, except in an approved Computer Refurbishment Program.
- No inmate shall have access to, or possesion of, any telecommunication capability, including Internet accessible computers, wireless devices such as pagers, or handheld computing devices, or cell phones.
- There shall be no inmate access to a computer outside the inmate's authorized work, vocational, or educational areas, unless approved by the ISO.

49020.18.4 Operation of Computer Programs Created by Inmates

Any computer-based system that was created by inmate programmers that is used to accomplish or complete CDC-related work shall not be operated or maintained by any inmate.

49020.18.5 Supervision of Inmates Using Computers

The persons responsible for supervising inmates’ use of computers shall certify in writing that these policies are being adhered to at their specific site.

A copy of this certification shall be kept on site by the local ISC.

49020.18.6 Education Computers

The use of computers for academic and vocational education is subject to the same requirement of due care applying to all personnel that use computers within applicability of the Department's information security and risk management program.

49020.18.7 PIA Systems

Inmate use of computers in PIA and in CDC facilities shall be in accordance with the departmental policies and institutional procedures.

49020.19 Information Security-Warnings

All critical Department systems shall display a warning at the first screen that any user of the system will see when the computer system is accessed.

49020.20 CDC E-Mail

CDC maintains an e-mail system to facilitate business communications and assist employees in performing their daily work activities.

The purpose of this section is to establish guidelines for the administration, maintenance use of the CDC e-mail system.

49020.20.1 Access to E-mail

CDC staff may be provided an ID for access to e-mail, either on the CDC Network or through an Internet Service Provider (ISP) if the CDC Network is not available. All access to e-mail shall be protected by password, and all policies pertaining to the use and protection of passwords shall apply. No generic or group access to an ID shall be used. A “group mailbox” is acceptable, as long as each individual in the group has their own ID and password.

If you require someone in addition to yourself to access or monitor your e-mail, establish a rule to forward/copy your mail to another’s mailbox. Sharing a password for any reason is prohibited.

49020.20.2 Acceptable Use

The e-mail system is provided for official CDC business. Using e-mail in an inappropriate manner may result in loss of e-mail privileges and/or disciplinary action.

Examples of appropriate use of the CDC e-mail system include, but are not limited to, the following:

- Scheduling, coordinating, and documenting business meetings and/or assignments.
- Notifying CDC personnel of changes in work policies and/or work procedures after the appropriate approval process has been completed (shall be followed up in writing).
- Transmitting and/or sharing nonconfidential work related material, including ducments, files, reference material, and links to Internet sites.
- Sending and receiving business related Internet mail.
- Notifying employees of CDC sanctioned employee events including, but not limited to, the Medal of Honor ceremony, United California State Employees Campaigns, and similar, approved activities.
- Scheduling appointments including personal appointments and lunch breaks on an electronic calendar.

49020.20.3 Unacceptable Use

Examples include, but are not limited to, the following:

- Using the system to discuss, distribute, or share confidential information.
- Reviewing, receiving, and/or intercepting the electronic communications of another employee without express, advance authorization by the employee or their management.
- Logging on with a user ID and password other than your own.
- Copying or routing notes, messages, documents, or memoranda to individuals who are not involved in the relevant work project or who otherwise have no business related interest in the subject matter of the note, message, document, or memorandum.
- Creating or sending notes or messages of a predominantly personal nature, or for personal gain.
- Except as otherwise provided in this policy, reading e-mail of another employee without their knowledge and consent.

- Sending sports pool or other forms of gambling messages.
- Using e-mail for any unlawful or illegal endeavor.
- Soliciting or advertising for non-CDC activities, including fundraising or items of a political nature.
- Allowing access to inmates or parolees, or sending messages on behalf of inmates or parolees.
- Transmitting profanity, obscenity, threatening language, gossip, or derogatory remarks.
- Distributing jokes, poems, chain-letters, or other nonbusiness related material.

49020.20.4 Privacy and Confidentiality

All e-mail is subject to unannounced inspections, and should be treated like other shared filing systems. E-mail is not private and is subject to monitoring with or without notice.

49020.20.5 Personal Information

Employees shall not seek out or use personal information maintained by CDC for their own private interest or advantage. Personal information shall not be transmitted in e-mail or as attachments to e-mail. Confidential information shall not be transmitted via e-mail.

49020.20.6 Chain Letters, Jokes and Other Non-CDC E-Mail

Chain letters and e-mail containing religious, humorous, and political messages are forbidden. E-mail that contains promises, hoaxes, or threats shall not be distributed. Receipt of such e-mail should be reported to management. Forwarding of non-CDC e-mail is forbidden. It is recognized that recipients cannot control in-coming mail. Use of CDC e-mail for personal matters should be kept to a minimum. Personal e-mail is discouraged.

49020.20.7 Offensive Content

E-mail shall be free of offensive or unlawful material, including slanderous, discriminatory, sexual, pornographic, profane, or revolutionary content. This prohibition applies to e-mail attachments and to the content of Internet sites referenced or linked from e-mail. Displaying, printing, disseminating or possession of such material may be reason for disciplinary action.

49020.20.8 Copyrighted Material

Use of CDC e-mail system to distribute copyright-protected material such as photographs, graphics, music, documents, etc., constitutes copyright violation, and may result in disciplinary action taken.

49020.20.9 Unsolicited E-Mail

Unsolicited e-mail may carry viruses. If the sender's identity and intent cannot be verified, such e-mail should be deleted unopened. Unsolicited e-mail from unknown senders should always be deleted unopened. Do not open attachments or Internet links accompanying such unsolicited e-mail.

49020.20.10 Use of Global Distribution Lists

Use of the global distribution list should be limited to departmental, state, or national emergencies, and information from executive levels or program areas that affect all employees. Distribution of conformation not required by all employees should be limited to the affected work groups or physical locations.

49020.20.11 Incoming E-Mail

It is realized that recipients cannot control incoming e-mail. Use of CDC e-mail for personal matters is discouraged where and when possible.

49020.20.12 E-Mail Administration

ISD shall perform all administration functions including, but not limited to, establishment of server mailboxes, system-wide filters, and virus scanning functions. ISD shall determine the disk space required to ensure correct functionality of the e-mail system. Staff are strongly encouraged to move messages from their "server inbox" to their "personal folders" if retention is required. Retention of e-mail is governed by CDC document retention policies.

49020.20.13 E-Mail Virus Protection

ISD shall manage the virus protection program for all workstations, servers, and network devices. All workstations connected to the CDC Network or are Internet-Accessible shall have the most current Virus Protection software, determined by ISD. CDC Network workstations shall be configured to automatic update of the virus protection software. Staff shall not disable or turn off this feature. Distribution of virus-laden e-mail may result in performance degradation of the CDC network and the removal from the network of the workstation(s) from which the infected e-mail is sent.

49020.20.14 Additional E-Mail Usage Guidelines

Local operating procedures and guidelines may apply to e-mail content and handling. These local guidelines and procedures are in addition to this e-mail policy, and may not be in conflict with or contradictory to this policy.

49020.21 Electronic Document Management

CDC is committed to ensuring that all departmental electronic documents, including e-mail messages, used by staff in the course of their employment are retained efficiently and in compliance with the Records Management Act, GC, § 14740, et seq.

49020.21.1 Retention Schedules

In its statewide departmental Records Retention Schedule (RRS) (DOM, Chapter 1, Article 23, Records Retention), CDC sets the time periods after which State documents are destroyed. This policy clarifies that the RRS extends to all electronic documents of CDC, including all e-mail messages and attachments to e-mail. These electronic documents include, but are not limited to, word processing files, spreadsheets, PowerPoint© presentations, and other computer displays.

Electronic documents stored both on local computers and network servers shall be deleted in accordance with the RRS, under the same time period that paper printouts of the documents would be disposed. Staff shall also, to the extent possible, delete all state electronic documents from stand-alone computer hard drives in accord with the RRS.

49020.21.2 E-Mail Retention

All opened e-mail shall be deleted from the CDC statewide server after 30 days, and unopened e-mail shall be deleted after 90 days. Once it is deleted, e-mail cannot be retrieved from the server.

To preserve sent or received e-mail messages, staff may save those messages into personal folders within the e-mail program, or elsewhere on their computer hard drive, or print them. Failure to move e-mail messages from the server will result in their automatic deletion from the server within the time frames noted above. Removal of e-mail from the server will not affect the contents of any personal folder. Staff is encouraged to save to a personal folder any e-mail messages that have an administrative, legal, or fiscal function related to their current work assignment. Those e-mail messages should then be deleted from the personal folders in accordance with the RRS.

49020.21.3 Reassignment of Workstations

The local computer coordinators shall erase all electronic documents from the hard drive of a computer once any staff member of CDC has ceased using that computer. All forms of electronic documents that the previous staff member created, received, or used shall be removed. As needed, the electronic documents may be transferred to another computer.

49020.22 Revisions

The Deputy Director, Policy and Evaluation Division, or designee shall be responsible for ensuring that the contents of this article are kept current and accurate.

49020.23 References

The Constitution of the State of California, Article 1, Section 1.

The Information Practices Act of 1977, Civil Code § 1798.

The Federal Copyright Act of 1976.

The California Public Records Act.

PC, § 502.

SAM, §§ 1601-1699, 4820, 4841,4841.3, 4842.1, 4989.7, 4990.1.

GC §§ 1222, 6250-6265, 14740-14770.

DOM §§ Chapter 1, Article 23, and Chapter 4, Articles 31, 40, 41, 45, 46, 48.