



INFORMATION SECURITY POLICY



Prepared by the
Information Security Office
January 31, 2003

TABLE OF CONTENTS

1.0 FOREWARD 1

2.0 INTRODUCTION 1

2.1 What is information security? 1

 2.1.1 What is information? 1

 2.1.2 What are information assets? 1

 2.1.3 What are privacy rights? 1

 2.1.4 What is business continuity? 1

 2.1.5 What is information security? 1

2.2 Why is information security necessary? 2

2.3 How were security requirements established? 2

2.4 How were security risks assessed? 2

2.5 How were security controls selected? 2

2.6 What was the information security strategy? 2

3.0 INFORMATION SECURITY 2

3.1 Information Security Policy (ISP) Document 2

 3.1.1 Purpose 2

 3.1.2 Scope 3

 3.1.3 Objective 3

 3.1.4 Management intent 3

 3.1.5 Supportive information security policies 3

3.2 ISP review and evaluation 3

3.3 Policy enforcement 3

4.0 ORGANIZATIONAL SECURITY 4

4.1 Information security infrastructure 4

 4.1.1 Information security management 4

 4.1.2 Information security coordination and oversight 4

 4.1.3 Summary of information security responsibilities 4

 4.1.4 Evidence of compliance requirements 4

 4.1.5 Authorization process for new facilities 4

 4.1.6 Authorization process for new agreements and contracts 4

 4.1.7 Specialist information security advice 5

 4.1.8 Cooperation between organizations 5

 4.1.9 Independent review of information security 5

4.2 Security of third party access 5

 4.2.1 Responding to access requests 5

 4.2.2 Identification of risks from third party access 5

 4.2.3 Types of access 5

 4.2.4 Reasons for access 6

 4.2.5 Third party access controls 6

5.0 ASSET CLASSIFICATION AND CONTROL 6

5.1 Accountability for assets 6

5.2 Information classification 6

 5.2.1 Confidential information 6

 5.2.2 Sensitive information 6

 5.2.3 Public information 7

6.0 PERSONNEL SECURITY 7

6.1 Security in job definition and human resources 7

 6.1.1 Documented information security responsibilities 7

6.1.2	Manager and supervisor responsibilities.....	7
6.1.3	Confidentiality agreements	7
6.1.4	Information access responsibilities	7
6.2	Information security awareness, training, and education (SATE).....	7
6.2.1	Management information security training	7
6.2.2	Individual information security training	8
6.3	Addressing information security incidents and malfunctions	8
6.3.1	Reporting information security weaknesses or threats	8
6.3.2	Reporting information system malfunctions	8
6.3.3	Reporting information security incidents	8
6.3.4	Responding to incidents.....	8
6.3.5	Learning from incidents.....	9
6.3.6	Disciplinary process	9
7.0	PHYSICAL AND ENVIRONMENTAL SECURITY	9
7.1	Secure areas	9
7.1.1	Secure area protections	9
7.1.2	Isolated delivery and loading areas.....	10
7.2	Equipment security	10
7.2.1	Equipment location and protection.....	10
7.2.2	Power protection	10
7.2.3	Cabling security	10
7.2.4	Equipment maintenance	10
7.2.4.1	Equipment physical maintenance	10
7.2.4.2	Equipment logical maintenance	11
7.2.5	Security of equipment off-premises.....	11
7.2.6	Secure movement, inventory, disposal, and reuse of equipment and media.....	11
7.3	Desk and work area controls	11
8.0	COMMUNICATIONS AND OPERATIONS MANAGEMENT	11
8.1	Operational procedures and responsibilities	11
8.1.1	Input data validation	12
8.1.2	Information transmission authentication.....	12
8.1.3	Verification of service delivery.....	12
8.1.4	Housekeeping (system backup, logging, etc.)	12
8.1.5	Operational change control	12
8.1.6	Incident management procedures.....	12
8.1.7	Separation of duties	12
8.1.8	Separation of development and production	12
8.1.9	External facilities management	12
8.1.10	Capacity monitoring	12
8.2	Software security	13
8.2.1	Control of system software.....	13
8.2.2	Control of applications software	13
8.2.3	Control of malicious software and hoaxes	13
8.3	Communications security	14
8.3.1	Security of communications devices	14
8.3.2	Security of network communications.....	14
8.3.2.1	Individual access controls	14
8.3.2.2	Technical access controls	15
8.3.2.3	Electronic commerce and E-government controls	15
8.4	Media handling and security	15
8.4.1	Media handling procedures.....	15
8.4.2	Management of removable computer media.....	15
8.4.3	Media and equipment disposal	15

9.0	ACCESS CONTROL	16
9.1	Business requirement for access control	16
9.2	Individual access management	16
9.3	Individual responsibilities	16
9.4	Network access control	16
9.5	Operating system access control	16
9.6	Application access control	16
9.6.1	Information access restriction	16
9.6.2	Sensitive system isolation	16
9.7	Monitoring access and use	16
9.8	Mobile computing	17
10.0	AUTOMATED SYSTEMS DEVELOPMENT AND MAINTENANCE	17
11.0	CONTINUITY PLANNING MANAGEMENT	17
11.1	Aspects of continuity planning	17
11.2	Business impact analysis	18
11.3	Writing and implementing continuity plans	18
11.4	EDD Continuity Plan for Business (CPB)	18
11.5	Business continuity testing and maintenance	19
11.6	Emergency Response and Business Continuity Training	19
11.7	Business continuity planning activation	19
12.0	COMPLIANCE	20
12.1	Compliance with requirements	20
12.1.1	Copyright and Intellectual property rights	20
12.1.2	Security of confidential and sensitive information	20
12.1.3	Misuse of information processing technology	20
12.1.4	Regulation of cryptographic controls	20
12.1.5	Collection of evidence	20
12.2	Reviews of security policy and technical compliance	21
12.2.1	Compliance with security policy	21
12.2.2	Technical compliance checking	21
12.3	System audit considerations	21
12.3.1	System audit controls	21
12.3.2	Protection of system audit tools	21
12.4	External auditor access	21
APPENDICES		22
APPENDIX A - STATUTORY AUTHORITY		22
California state laws		22
California state administrative policies		23
Federal laws		23
APPENDIX B - INTERNATIONAL STANDARD - 17799 SUMMARY		24
APPENDIX C - INFORMATION SECURITY POLICIES		25
APPENDIX D - SUMMARY OF INFORMATION SECURITY RESPONSIBILITIES		26
Individuals with access		26
EDD employee		26
Managers and supervisors		26
Branch management		26
Information Technology Branch (ITB)		26
Information Security Officer (ISO)		26
Business Operations and Planning Support Division (BOPSD)		27

Audit and Evaluation Division (A&ED)	27
Investigation Division, Internal Affairs Unit	27
Human Resources Services Division (HRSD)	27
APPENDIX E - EVIDENCE OF COMPLIANCE	28
Each local office:.....	28
Each branch:.....	28
All developers and maintainers:.....	28
Information Security Office:	28
Business Operations Planning and Support Division (BOPSD):.....	28
Audit and Evaluation Division (A&ED):	28
Human Resources Support Division:.....	28
APPENDIX F - EDD MAJOR SYSTEMS	29
APPENDIX G - INFORMATION LABELING AND HANDLING.....	30
APPENDIX H - INFORMATION SECURITY TRAINING REQUIREMENTS	32
APPENDIX I - DEVELOPMENT AND MAINTENANCE SUPPORT	33
I.1 Planning documentation.....	33
I.2 General design documentation.....	33
I.3 Detail design documentation	33
I.3.1 Risk analysis and impact assessment	33
I.3.2 Risk mitigation plan.....	34
I.3.3 Implementation plan.....	34
I.3.4 Operating procedures	34
I.3.5 Test plan	35
I.3.6 Operational change control plan	35
I.3.7 Capacity planning and monitoring plan.....	35
I.3.1 System and information backup.....	35
I.3.2 Operator, event, transaction, network, and system logs.....	35
I.3.3 Data validation	36
I.4 Development and maintenance controls	36
I.4.1 System Testing	36
I.4.1 Protection of system test data.....	37
I.4.2 Separation of development and production systems	37
I.4.3 Access control to program source library.....	37
I.4.4 Technical review of system software maintenance.....	38
I.4.5 Using cryptographic tools.....	38
I.4.6 Outsourced development.....	38
I.4.7 Outsourced acquisitions.....	38
I.4.8 Restrictions on changes to commercial software packages	39
I.5 Acceptance of information security controls	39
I.6 Application retirement	39
APPENDIX J - SAMPLE MESSAGES	40
Sample security access warning message	40
Sample web disclaimer message	40
APPENDIX K - REFERENCES.....	41
GLOSSARY	42

1.0 FOREWARD

The Employment Development Department (EDD) has successfully delivered services for over 60 years. More than 1 million employers and 19 million wage earners and their families now rely upon EDD to deliver unemployment compensation, disability insurance, workforce investment, labor market information, job service, and employment payroll tax and wage collection services. More than 11,000 people in over 400 service points throughout California make up the EDD team that delivers these essential services. Meeting program delivery mandates requires a timely flow of accurate information. That flow of often very sensitive and confidential information depends upon the public trusting EDD to keep their information secure.

To continue that trust, EDD program success, and security of EDD information assets, this overarching policy addresses each major aspect of information security in a separate section. Each section starts with an identification box that contains a policy statement that provides overall direction for all EDD staff and information users. The detail in each section provides general and specific detailed requirements to comply with that security component. The appendices support this policy with administrative and legal requirement references, a glossary of relevant terms, samples, and the specific additional information security requirements for those who develop and maintain EDD's systems, networks, and computers.

2.0 INTRODUCTION

2.1 What is information security?

Information security protects information assets from a wide range of threats to ensure privacy and business continuity.

2.1.1 What is information?

Information is a collection of meaningful data that records numbers, timing, values, events, historical facts, and other related data. Whatever the form information takes and whatever the means used to share information, information is the data conveyed, not the paper, tape, disk, or other technology used for processing, storage, or sharing.

2.1.2 What are information assets?

EDD information assets include all employer payroll tax and wage reports, personal work history, and all other information gathered and used by EDD programs. Information assets also include the media, systems, applications, equipment, and facilities used to collect, store, manage, process, and share information.

2.1.3 What are privacy rights?

Privacy rights are legal and administrative mandates that require protecting individual and employer information from inappropriate disclosure.

2.1.4 What is business continuity?

Business continuity means the ongoing delivery of consistent, timely, accurate services with the ability to rapidly restore services following a disruption.

2.1.5 What is information security?

Information security means:

- a) **Confidentiality:** Protecting privacy by limiting access to those with a legal right for access and a legitimate business need-to-know, and by protecting information assets against loss, and unauthorized or accidental access, use, alteration, modification, destruction, or disclosure;

- b) **Integrity:** Safeguarding the accuracy, reliability, and completeness of information and information processing methods by providing oversight, logging, documentation, and other controls that verify the timely accurate delivery of information and services; and,
- c) **Availability:** Ensuring the availability of information, information systems, and applications to authorized individuals when and where needed.

2.2 Why is information security necessary?

Oversight agencies, administrative policy, and the law (see Appendix A - Statutory Authority) mandate information security to protect confidentiality, privacy, and service delivery.

2.3 How were security requirements established?

Legal and administrative mandates set most of the information security controls that EDD must follow. These mandates also require ongoing formal risk assessment to identify and address any new or additional threats and vulnerabilities that may prevent EDD from achieving its mission.

2.4 How were security risks assessed?

The EDD continually assesses exposures to ensure its information security controls remain suitable and effective. With the move to deliver interactive services directly to customers over public networks and the Internet, EDD conducted a risk assessment (see Glossary) with expert contractor guidance to identify and address additional exposure with appropriate controls.

2.5 How were security controls selected?

The EDD Information Security Office (ISO) worked closely with its internal business partners and with EDD control agencies to refine and develop these controls into cost-effective measures to eliminate or minimize potential disruptions and damages.

2.6 What was the information security strategy?

The ISO followed its consultants' recommendations to consolidate and organize its information security requirements by following the worldwide information security standard (see Appendix B - International Standard - 17799 Summary). This standard used by the United States government and most other large organizations provides a rigorous approach and template to develop a comprehensive information security policy. It builds into the result review and updating requirements to keep the policy current and effective.

3.0 INFORMATION SECURITY

Information security policy statement:

Each individual authorized access to EDD information, systems, applications, equipment, facilities, and other information assets must follow EDD information security policies and good business practices to protect those assets from unauthorized access, use, modification, deletion, destruction or disclosure.

Each EDD employee must help prevent, detect, report, and minimize compromise to any information asset. They must help preserve business continuity, protect the health and safety of customers and staff during a disruption, and following a disruption carry out their duties to assist with the rapid prioritized restoration of services.

3.1 Information Security Policy (ISP) Document

3.1.1 Purpose

This policy sets the minimum information security standards to protect EDD information, communications, networks, systems, applications, equipment, facilities and other information assets.

3.1.2 Scope

This policy consolidates the many existing legal and administrative information security requirements with agreed upon internal controls into a single departmental policy.

3.1.3 Objective

This policy defines and communicates departmental information security roles, responsibilities, processes, and procedures to all users of EDD information assets.

3.1.4 Management intent

This policy reflects the Director's commitment to maintain consistent and effective information security across the organization. All EDD management levels endorse and enforce this policy.

3.1.5 Supportive information security policies

Senior management requires and approves any supportive information security policies that all information users must follow to protect EDD information assets (see Appendix C - Information Security Policies).

- a) The ISO provides detailed departmental administrative information security policies;
- b) The Information Technology Branch (ITB) with ISO oversight provides detailed departmental technical information security policies; and,
- c) Branches and local offices provide specialized local information security policies.

3.2 ISP review and evaluation

The ISO keeps the ISP current with:

- a) Changes in laws, rules, regulations, administrative requirements, and business needs;
- b) Branch feedback from their annual information security reviews and business continuity testing;
- c) The policy's effectiveness, as demonstrated by the nature, number, and impact of information security incidents;
- d) The effects of changing technology on information security; and,
- e) The cost and impact of controls on ongoing business efficiency.

3.3 Policy enforcement

Any unauthorized access, use, disclosure, modification, or deletion of confidential or sensitive information, or any inappropriate or illegal use of State owned hardware, software, networks, or communications is subject to progressive corrective disciplinary and formal adverse action that may include dismissal, civil prosecution, and criminal prosecution.

The State prosecutes to the maximum extent permitted by law any individual that illegally or inappropriately discloses confidential or sensitive information, or who disrupts EDD business operations through a violation of security policies or legal requirements. Contract staff who violate the terms of their contracts or non-disclosure agreements expose themselves and their employers to additional prosecution and penalties.

Anyone who wrongfully discloses confidential health or medical diagnosis information in violation of the Health and Insurance Portability and Accountability Act of 1996 (HIPAA) may incur further sanctions:

Criminal Offense Penalties	HIPAA Sanction	Prison Term
Wrongful Disclosure	\$50,000 per offense	1 year
Wrongful Disclosure under false pretenses	\$100,000 per offense	5 years
Wrongful Disclosure with intent to sell, transfer, or use	\$250,000 per offense	10 years
Civil Offense Penalties	\$100 to \$25,000 per violation per year	

4.0 ORGANIZATIONAL SECURITY

Organizational security policy statement:

The EDD information security program utilizes centralized management and reporting with decentralized implementation and oversight.

4.1 Information security infrastructure

4.1.1 Information security management

All members of the EDD management team share the responsibility to consistently and effectively manage information security and the continuity of business operations. This policy documents the EDD standards to protect information assets and business continuity. Each manager must document in a risk assessment the information assets utilized in their areas, all potential risks to those assets, and identify the most cost-effective controls to address those risks. Each manager must prepare and maintain a local information security policy that documents any additional needed local controls to address those risks. The ISO must approve those controls, and the ITB must approve any technology or technology controls.

4.1.2 Information security coordination and oversight

- a) The ISO serves as the central contact point for departmental information security standards, oversight, coordination, incident response, and incident reporting;
- b) The ITB provides availability, management, oversight, monitoring, protection, and standards for EDD enterprise information technology, network, and communications assets;
- c) Each Branch provides all branch personnel and sites with information security direction, coordination, oversight, resources, and testing validation; and,
- d) Each office manager ensures staff training and provides direct oversight and information security assessment, planning, documentation, testing, maintenance, and coordination.

4.1.3 Summary of information security responsibilities

Every individual and organization with access to EDD information assets must protect those assets (see Appendix D - Summary of Information Security Responsibilities).

4.1.4 Evidence of compliance requirements

Legal and administrative mandates require EDD to record and maintain documented evidence of information security compliance for auditing purposes (see Appendix E - Evidence of Compliance).

4.1.5 Authorization process for new facilities

Each branch must obtain ISO, ITB, and Business Operations and Planning Support Division (BOPSD) approval before activating any new facility. The ISO provides overall information security advice. The ITB coordinates information technology, network, and communications security. The BOPSD coordinates implementation of physical security with contractors and the Facilities Management Group within the California Department of General Services.

4.1.6 Authorization process for new agreements and contracts

The Branch Deputy Director or Directorate must approve all contracts, service agreements, third party business partner agreements, and outsourcing agreements. EDD's internal clearance process requires review by the BOPSD Procurement Section, the Legal Office, the ITB, and the ISO. These clearances verify the completeness of the risk assessment and inclusion of the appropriate controls in the contract or agreement. They verify that a contractor representative authorized to sign vendor contracts has signed the contract or agreement committing the vendor

to adhere to the EDD information security policy. They verify that agreement includes appropriate personnel screening, training, and supervising protections for all vendor staff who will receive access to EDD sensitive or confidential information. They verify the contractor will provide EDD with the written results of their screening before permitting access. They verify the contractor will have each vendor staff member who will access EDD sensitive or confidential information sign a Confidentiality Statement (DE 7410).

4.1.7 Specialist information security advice

The ISO provides the Department with expert advice on information security policy, practices, and controls. The ITB works closely with the ISO, the HHSDC technical staff, State control agencies, and information security contractors to provide the Department with a ready source of expert technical security guidance information and advice. The BOPSD provides the Department with expert advice on physical and facility security.

4.1.8 Cooperation between organizations

The ISO provides the central EDD contact point to provide information security cooperation with other organizations. As part of this cooperative effort and to help keep EDD information security current and effective, the ISO participates in information security sharing and forums with federal, state, county, city, private, and emergency service provider organizations.

4.1.9 Independent review of information security

The ISO, ITB, Program Review Branch, and Audit and Evaluation Division provide internal review and monitoring of EDD information security. The U.S. Department of Labor, control agencies, and independent contractors periodically provide external information security review. Review findings with corrective action and continuous improvement opportunity recommendations go to the Director.

4.2 Security of third party access

Each manager who contracts for or oversees third party access to EDD information assets must ensure the ongoing security of that access. Third parties include all individuals, independent contractors, government agencies, or business entities not employed by the EDD who assist in the conduct of EDD business functions or provide the EDD with goods or services.

4.2.1 Responding to access requests

Employees must immediately send all third party requests for:

- a) General information to the Communications Director (public information officer);
- b) Data for law enforcement agencies investigating a felony to the Investigation Division; and,
- c) All other sensitive or confidential information to the data owner or the ISO.

4.2.2 Identification of risks from third party access

Before allowing third party access to EDD sensitive or confidential information managers must document in a risk assessment all potential risks and the controls to address those risks. The ISO must provide advance approval of those controls. The ITB must provide advance approval of any technology or technology controls used to enable and secure automated information access.

4.2.3 Types of access

Third parties requesting information access must clearly identify the type of access requested, and when applicable, the length of time they will require access. Requests may require access to facilities, filing cabinets, telecommunications closets, paper files, printed materials, reports, manuals, and other EDD documents, or to automated files and databases. Most access requests involve compliance with legal and administrative requirements. These mandates require EDD to

provide timely response to requests for information from third parties and permit recovery of certain costs incurred from responding. The ISO maintains service contracts with third party requesters to provide bulk and multiple information requests.

4.2.4 Reasons for access

Before granting access to sensitive or confidential information managers must verify the third party possesses legal access authorization and demonstrates a valid business need; e.g., access needed to make repairs, business partner delivery mandate, or contract requirements.

4.2.5 Third party access controls

Managers must control, monitor, and when appropriate, escort third party staff. In lieu of providing escort, managers may authorize contractor access provided they:

- a) Use a screening process equivalent to EDD human resource requirements to ensure each individual does not pose an unmanageable security risk;
- b) Inform each individual of their information security responsibilities; and,
- c) Have each individual sign an appropriate Confidentiality Statement (DE 7410) to formally agree to abide by this policy and protect EDD's information assets.

5.0 ASSET CLASSIFICATION AND CONTROL

Asset classification and control policy statement:

The EDD requires the inventory of every information asset and the assignment of a data owner to each asset. The data owner must classify and oversee the protection of each asset in accordance with the value of that asset.

5.1 Accountability for assets

Ownership, inventory, and accountability for each information asset belongs to the branch that owns the major system or that primarily collects, maintains, and uses that information (see Appendix F – EDD Major Systems). Branches who share information assets must coordinate to ensure inventory and security of shared assets. Regardless of ownership, each manager and supervisor must ensure the protection all information assets used in their areas.

5.2 Information classification

All EDD information must be identified and classified as public, sensitive, or confidential, then protected in accordance with its classification (see Appendix G – Information Labeling and Handling). All individuals must know the classifications of the information they use and the protections they must provide.

5.2.1 Confidential information

Confidential information includes all information exempt from public disclosure as established by law or contractual agreement. Confidential information includes all data associated with a person or an employing unit and all identifying information; e.g., name, address, telephone number(s), Social Security number, and employer identification number(s).

5.2.2 Sensitive information

Sensitive information includes all information except confidential information which, if inappropriately released, used, or modified, could jeopardize the integrity of a system or program or compromise EDD's ability to carry out its business functions. A few examples include financial transactions, all regulatory actions, computer programs, copyrighted items, software, and EDD business related documents; e.g., internal audit reports, logon procedures, network configuration diagrams, database schemas, and sensitive portions of procedural manuals.

5.2.3 Public information

Public information includes all information not classified as sensitive or confidential that EDD prepares, owns, uses, or retains; e.g., directives, manuals, miscellaneous publications, and data with confidential and sensitive information removed.

6.0 PERSONNEL SECURITY

Personnel security policy statement:

The EDD will reduce the risk of human error, theft, fraud or misuse adversely affecting EDD information assets and business continuity.

6.1 Security in job definition and human resources

6.1.1 Documented information security responsibilities

Managers must document local information security responsibilities, preferably in job definitions, and inform each individual of their departmental and local information security responsibilities.

6.1.2 Manager and supervisor responsibilities

Managers must ensure training of each individual, including contractor and vendor staff, who works in their areas and provide oversight to ensure adherence to EDD information security policies and compliance with the incident reporting process. Managers will provide appropriate screening in the recruitment process. Managers must provide additional controls as needed to secure the activity of those who oversee or perform sensitive activities; e.g., funding or benefits, modifying systems, approving contracts, modifying automated access rights, and accessing personal information.

6.1.3 Confidentiality agreements

Managers must ensure that all staff, contractors, and others under their oversight agree in writing to protect information assets and comply with EDD information security requirements. Each must sign a Confidentiality Statement (DE 7410) (non-disclosure) agreement before receiving access to sensitive or confidential information. Managers must file and maintain the signed DE 7410 forms (see Administrative Manual, Attendance Clerk Handbook Sections 4-1350 to 4-1359).

6.1.4 Information access responsibilities

Managers must explain the responsibilities for each authorization or access mechanism issued; e.g., keys, card keys, and passwords. Managers must follow the EDD Administrative Manual, Attendance Clerk Handbook Sections 4-1360 and 4-9300 procedures to document each access mechanism issued on each individual's own Appointment / Separation Clearance Checklist, form DE 7411. Managers must use this checklist to ensure revocation or return of all authorizations and access mechanisms when an individual transfers within or separates from EDD.

6.2 Information security awareness, training, and education (SATE)

Each individual must complete introductory and annual refresher security awareness, training, and education (SATE). This training must cover both their departmental and local information security responsibilities as defined in Appendix H - Information Security Training Requirements.

6.2.1 Management information security training

Managers must stay current in their training to oversee departmental and local information security. They also must stay current in their training to effectively develop, document, maintain, test, and oversee any required local information security policies, training materials, and local business continuity planning.

6.2.2 Individual information security training

Managers must ensure each of their EDD employees receive initial and annual refresher information security training. This training must cover local and departmental requirements. The ISO information security training SATE module meets departmental training requirements. Managers must provide any required additional local information security training and document training currency in a local training completion log. Managers must preclude access to sensitive or confidential information before training completion. They also must revoke access if annual refresher training lapses.

6.3 Addressing information security incidents and malfunctions

Each individual authorized information access must help limit damages by quickly detecting, addressing, and reporting to their manager any actual or potential security incidents, threats, weaknesses, or malfunctions.

6.3.1 Reporting information security weaknesses or threats

Security weaknesses and threats include potential exposures; e.g., unattended workstations left connected to secure systems, shared or exposed passwords, secure workstations left available for public access or viewing, suspected malicious software, viruses, or denial of service attacks, inappropriate e-mail, and unrecognized or suspicious e-mail. Employees must not attempt to investigate or prove a suspected weakness because such attempts could disrupt operations and may in themselves constitute an information security incident. Managers must report security weaknesses to their deputies who will share concerns that could adversely affect the Department with the ISO.

6.3.2 Reporting information system malfunctions

Malfunctions include the failure of automated systems, computer, communications, and network technology, or physical protections; e.g., inoperable card key actuated door. Each manager must coordinate repair and report to the ISO any malfunction that is also an information security incident.

6.3.3 Reporting information security incidents

Managers must immediately notify the ISO of any information security incident and follow up within one business day with a written Security Incident Report, DE 7413 (see EDD Security Incident Reporting Policy and EDD Privacy Policy). Support personnel who assist with repairs must assist in completing the technical portions of the security incident report. Information security incidents include:

- a) Unauthorized access or other breach of information confidentiality, integrity, or availability;
- b) Any unauthorized or accidental inspection, access, use, modification, tampering, or destruction of confidential or sensitive information;
- c) Any violation of EDD information security policies, practices, or procedures; and,
- d) Any actual computer virus infection, input flooding that ties up system resources (denial of service attack), or serious information system failure resulting in extended loss of services.

6.3.4 Responding to incidents

As the central EDD coordinator for all information security incident resolution, the ISO:

- a) Intakes, investigates, and coordinates EDD information security incident responses while keeping senior management informed;
- b) Provides customer feedback, and prepares mandated control agency reports;
- c) If an incident involves inappropriate disclosure of confidential information, the ISO coordinates the required notifications of affected individuals or entities; and,

- d) As needed, coordinates and convenes with the ITB a Security Incident Response Team (SIRT) to resolve technical incidents. The SIRT facilitates incident repair, documents detailed repair actions, and keeps the ISO informed during the recovery effort. During the repair efforts, only clearly identified and authorized SIRT members may access live systems and data. Under the direction of the ISO, the SIRT develops Security Advisories to notify System Administrators and/or all employees of required actions, repairs, or patches to preclude additional information security incidents.

6.3.5 Learning from incidents

The ISO monitors the types, volumes and costs of all reported information security incidents and malfunctions to identify and address significant threats and high impact trends. Upon management request or following significant incidents, the ISO also conducts a post-incident evaluation. That evaluation provides the feedback that the ISO uses to identify controls to prevent or mitigate future occurrences.

6.3.6 Disciplinary process

Anyone who creates an information security incident is subject to disciplinary action that may include civil and criminal prosecution (see 3.3 - Policy Enforcement).

7.0 PHYSICAL AND ENVIRONMENTAL SECURITY

Physical and environmental security policy statement:

Each EDD office manager must identify risks and implement suitable physical and environmental controls for all secure areas and information processing equipment to ensure information security and prevent opportunities for malicious or unauthorized activities.

7.1 Secure areas

Managers must implement appropriate controls to protect secure areas. Secure areas are any office, room, or facility; e.g., communication closets, computer rooms, backup depots, data collection areas, or off-site facility that houses or processes either sensitive or confidential information, or that contains EDD information processing equipment; e.g., computers, servers, communications, or network devices. EDD requires use of formal agreements that comply with department contract and security requirements for secure areas at facilities not operated by EDD, including the HHSDC.

7.1.1 Secure area protections

In addition to EDD employees, many different individuals access EDD secure areas, including:

- a) Hardware and software maintenance vendors;
- b) Cleaning, catering, movers, security guards, and other support service personnel;
- c) Student assistants and other casual short-term appointments; and,
- d) Consultants or other contractor staff.

Managers must protect all assigned secure areas:

- a) Work with the BOPSD to establish a clearly defined physical security perimeter using walls, locked doors, barriers, partitions, security guards, etc. to guard against unauthorized entry;
- b) Limit, authorize, verify the identity of each visitor, and supervise all access;
- c) Limit personnel access based on work assignments;
- d) Limit awareness and operational knowledge of secure areas on a need to know basis;
- e) Keep unstaffed secure areas locked and periodically checked;
- f) Regularly change secure area access mechanisms; e.g., keys, locking codes, and card keys;

- g) Appropriately provide each visitor to a secure area with advance warning of security requirements, log each visitor's arrival and departure, provide each a visitor badge, and provide escort supervision; and,
- h) Preclude any use of recording equipment in secure areas without prior management approval. Managers must directly oversee recording operations and personnel.

7.1.2 Isolated delivery and loading areas

As high traffic areas that frequently receive information and other items that must be secured, delivery and loading areas are considered secure areas. Local managers must protect these areas and the items that move through them with appropriate isolation, limiting individual access, logging deliveries, isolating and inspecting deliveries for potential hazards, and keeping unmonitored access doors locked.

7.2 Equipment security

7.2.1 Equipment location and protection

Managers must locate and appropriately protect communications, network, and information processing equipment:

- a) Locate equipment to minimize viewing and unnecessary access;
- b) Secure exposed equipment with locked areas, key locks, locking kiosks, locking cables, and secured docking stations, and regularly change those locks and access mechanisms;
- c) Protect all equipment in accordance with manufacturers' instructions; e.g., protect against x-rays, sunlight, shock, strong electromagnetic fields, humidity, dust, vibration, chemical effects, electrical supply interference, and excessive temperatures;
- d) Protect all equipment in hazardous or dirty environments with physical protections; e.g., keyboard membranes, dust covers, clean areas, or filtered cabinets;
- e) Control eating and drinking in and around equipment; and,
- f) Prepare for major disruptions in local or adjacent facilities; e.g., theft, fire, heat, smoke, water (flood or supply failure), explosion, sabotage, terrorist attack, and earthquake.

7.2.2 Power protection

Managers must prepare for and protect against power failures and electrical interruptions:

- a) Provide backup lighting and flashlights;
- b) Appropriately protect equipment with manufacturer approved uninterruptible power supplies (UPS) to provide a controlled, safe, and automatic shut down during a power failure;
- c) Ensure BOPSD locates and identifies power switches to facilitate emergency power down;
- d) Develop contingency plans to address electrical failure and failure of backup UPS devices;
- e) Periodically test and certify that UPS and power down procedures work as expected; and,
- f) Periodically test and certify the power recovery processes work as expected, including system restart and reconnection to local and wide area networks.

7.2.3 Cabling security

The ITB must ensure data and telecommunications cabling complies with EDD and industry standards for installation and protection (see EDD Wiring Guide, Specifications & Standards).

7.2.4 Equipment maintenance

7.2.4.1 Equipment physical maintenance

Managers must ensure proper and regular physical maintenance of all local information processing equipment in accordance with manufacturer recommended service intervals and specifications. State policy only permits authorized maintenance staff to conduct repairs and service equipment. Managers must request ITB to clear any sensitive and confidential

information before sending equipment away for maintenance. System administrators must maintain a written log of all maintenance and service activity.

7.2.4.2 Equipment logical maintenance

Managers must ensure regular logical maintenance of all local information processing equipment in accordance with ITB recommendations and industry best practices to include at a minimum:

- a) Maintain system software version levels as approved by the ITB;
- b) Maintain system software with current security patches;
- c) Scan all systems at least monthly to detect and repair bad sectors, and when necessary, reorganize disk drives; and,
- d) Maintain a written log of all maintenance and service activity.

7.2.5 Security of equipment off-premises

Managers must ensure appropriate security before permitting equipment off premises. Appropriate controls must address the risks that vary between locations; e.g., eavesdropping, theft, damage, and technical support. Those authorized to use equipment at home or for mobile computing must comply with State and EDD telecommuting and mobile computing requirements.

7.2.6 Secure movement, inventory, disposal, and reuse of equipment and media

Managers must comply with property accounting requirements to move, remove from local inventory, dispose, or reuse any surplus information technology equipment or media. Removal of information assets from an EDD facility without required prior written authorization constitutes an information security incident and crime. Managers must use a Permit to Remove Property From Building (DE-1738), for the temporary assignment, removal, and return of information assets from or to an EDD facility (e.g., for use of a laptop or personal digital assistant). Managers must also use an Equipment Requisition-Transfer Form, DE1904E to track any information technology assets moved from one cost center or location to another.

7.3 Desk and work area controls

Managers must enforce the Clean Desk Policy to prevent unauthorized information disclosure, and the Screen Saver Policy to automatically secure unattended workstations.

8.0 COMMUNICATIONS AND OPERATIONS MANAGEMENT

Communications and operations management policy statement:

The EDD will protect all operations and communications including supportive technology, e.g., networks and systems to acceptable levels of risk as defined by a risk assessment.

8.1 Operational procedures and responsibilities

Each office manager must document their risk assessment for the use of local communications, networks, and systems. That initial and ongoing risk assessments must provide the basis for each manager to develop, document, and maintain the information security controls in their local operating procedures and responsibilities. These procedures must detail any special local requirements for information intake, processing, communication, storage, handling, backup, recovery, and access. EDD classifies its documented operating procedures as sensitive, so managers must securely store this documentation, limit its access to only authorized individuals, log all changes, and ensure its protection when stored on or transmitted through public networks, preferably through encryption. Managers must require, oversee, and document annual or more frequent testing of backup and recovery procedures. This documentation including test results must remain available for auditing.

8.1.1 Input data validation

Managers must document and oversee their local procedures to ensure the confidentiality, integrity, and accuracy of all information accepted and entered into EDD programs.

8.1.2 Information transmission authentication

Managers must document and oversee their local procedures to authenticate an individual's identity and verify their legal right and business need before allowing access to sensitive or confidential information.

8.1.3 Verification of service delivery

To ensure successful service delivery and to minimize or resolve disputes, EDD requires verification with receipts, digital certificates, etc. for all transfers of money, sensitive information, or confidential information. Managers must keep all logs and verification materials secured.

8.1.4 Housekeeping (system backup, logging, etc.)

Managers must require and oversee regular housekeeping processes within their span of control; e.g., backup, logging, monitoring, tracking, etc.

8.1.5 Operational change control

Managers must ensure local operational changes do not disrupt business functions, cause information security incidents, or compromise existing controls.

8.1.6 Incident management procedures

Managers must document their local procedures for timely incident resolution and ISO notification to comply with the EDD information security incident procedures (see 6.3).

8.1.7 Separation of duties

Managers must oversee and separate duty functions to reduce the risk of an information security incident. They must separate approval, benefit determination, ordering, payment, acceptance, and inventory functions so no one individual or group may both order and approve expenditure for benefits, goods, contracts, or services.

8.1.8 Separation of development and production

Managers must ensure clear separation and oversight to keep development and testing activities from adversely impacting production.

8.1.9 External facilities management

External facilities include any facilities not operated by EDD and must receive equivalent protection as secure areas (see 7.1 Secure areas) if they process EDD sensitive or confidential information, or they house EDD information assets; e.g., communication closets, computer rooms, backup depots, data collection areas, etc. External facility contracts including with the HHSDC must mandate compliance with EDD information security requirements.

8.1.10 Capacity monitoring

Managers must ensure ongoing monitoring of their communications, networks, and systems to identify trends, address changing needs, and address emerging capacity problems before they adversely impact service delivery. They must address additional needs for hardware, software, communications, storage, capacity, and staff sufficiently far in advance to permit state timeframes for justification, approvals, funding, acquisition, contracting, delivery, installation, upgrade, personnel hiring, and personnel training without disrupting services.

8.2 Software security

8.2.1 Control of system software

System software includes all operating systems, databases, utilities, and tools used to develop, setup, test, run, monitor, and audit applications, communications, networks, servers, PCs, etc. Only those with the highest levels of security may access system software as that access permits complete control and access to all associated resources, communications, and information. Managers must limit system software access to those with the technical skills, an authorized business need, and only for the duration of that specific business need. The ITB provides ongoing monitoring and security of all centralized departmental system software. Managers must provide appropriate controls for all local system software and must limit access to those with an authorized business need and only for the duration of that specific business need.

8.2.2 Control of applications software

Application software includes all packaged and custom built programs other than systems software, such as word processors, spread sheets, database programs, Internet programs, web pages, and the custom computer programs used to support EDD business activities; e.g., UI, DI, Tax, JS, etc. The ITB provides ongoing monitoring and security of all centralized departmental application software. Managers must provide appropriate controls for all local application software and must limit access to those with an authorized business need and only for the duration of that specific business need.

8.2.3 Control of malicious software and hoaxes

Malicious software and hoaxes waste staff time, waste resources, and may compromise information assets by installing programs that permit unauthorized activity, monitoring, and access. Hoaxes and urban myths trick users through misinformation, misdirection, fear, or greed into making disruptive repairs and inappropriately spreading the hoax. The ISO and ITB requires and uses multiple layers of controls to limit exposure and prevent cyber terrorists from using malicious software and hoaxes to disrupt or compromise information services, communications, networks, systems, or assets:

- a) Only buying software programs and control routines from a reputable source;
- b) Whenever possible obtaining written assurances from the vendor that their product does not contain covert channels or Trojan code;
- c) Only using evaluated or appropriately certified products;
- d) Controlling access to, and modification of, those products once installed;
- e) Using staff and vendors of proven trust to work on departmental systems.
- f) Using third party independent validation and verification of work items produced;
- g) Providing ongoing filtering, anti-virus, and other protections against malicious software;
- h) Ensuring local computers automatically update anti-virus programs at least daily;
- i) Ensuring local computers automatically scan all incoming information, email, etc.;
- j) Ensuring local computers automatically perform a full system scan at least monthly to:
 1. Detect and remove viruses; and,
 2. Detect and remove spyware.
- k) Requiring managers to oversee staff to limit behaviors that increase these types of exposures;
- l) Isolating connections to public networks (see 8.3.2.1 Individual access controls);
- m) Utilizing documented agreements or contracts with the HHSDC, control agencies, and contractors to advise ITB whenever new malicious software or hoaxes require special protections or corrective measures;
- n) The ITB and ISO promptly notifying and sharing special protections or corrective measures with EDD system administrators and staff;

- o) System administrators promptly assisting their customers in implementing required protections or corrective measures; e.g., not opening e-mail attachments, turning off auto-execute features, and disabling networks; and,
- p) Keeping staff informed of current hoaxes and malicious software protections.

8.3 Communications security

Managers must ensure the secure, accurate, and timely completion of all information exchanges. All confidential information, software, financial, or other sensitive information, and any information sent over a public communications network, facsimile, Internet connection, via courier, etc. that does not have appropriate security is considered at risk. Managers must work with the ITB to implement appropriate controls for any information considered at risk. The ITB oversees and helps implement the controls that secure and verify exchanges considered at risk:

- a) Managers must provide individuals under their supervision with the training and oversight to ensure the proper, secure use of the communications means and equipment used; and,
- b) Third party contracts and software agreements must protect exchanges of information.

8.3.1 Security of communications devices

All individuals must appropriately use, protect, secure, report abuses, and comply with policies when using EDD communications devices; e.g., telephones, long distance, credit cards, cellular phone, voice mail, pagers, and interactive voice response (IVR):

- a) All EDD staff must recognize, avoid, and report telephone scams and fraudulent phone calls to their immediate supervisor or manager;
- b) All EDD staff must recognize, avoid, and report any abuse of their voice mail services to their immediate supervisor or manager;
- c) All EDD staff issued cellular telephones must follow the EDD Cellular Telephone Policy;
- d) Those responsible for IVR oversight must report abuses to the ITB telecommunications unit; e.g., flooding the service to make lines unavailable or tying up storage with recordings;
- e) All EDD staff must appropriately log their long distance telephone and credit card usage;
- f) Managers must carefully monitor charges and report inappropriate charges to their accounting manager;
- g) Managers must report equipment problems, equipment theft, and loss to the ITB Consolidated Services Help Desk; and,
- h) Managers must report loss of devices that contains sensitive or confidential information (includes personal telephone numbers) as information security incidents to the ISO.

8.3.2 Security of network communications

EDD reduces risks to its communications networks with human resource and technical controls:

8.3.2.1 Individual access controls

Managers must ensure all individuals in their areas comply with the Access Control Policy and the Employee Internet Access Policy. No one should install or use any physical or logical connection that bypasses EDD controls without advance written permission from the ITB Deputy Director and the ISO. Physical connections include modem, wireless, peer-to-peer, DSL, cable, or PC to PC, etc. Logical connections include personal e-mail accounts, on-line streaming connections for radio, TV, audio, music, video, data, stocks, etc., instant messengers, download programs for sharing files, FTP links to personal web pages, etc. These types of connections expose information assets to unauthorized access and malicious software, so their use without advance written permission constitutes a serious information security incident.

8.3.2.2 Technical access controls

The ITB and HHSDC install, maintain, manage, secure, oversee, monitor, and provide network controls, guidance, and technical support for EDD enterprise communications, networks, and systems. The ITB restricts access to system, network, and communication equipment. The ITB, carefully guards its few permitted external connections and filters content with communications controls; e.g., authentication and validation systems, firewalls, routers, switches, virus scanners, network analyzers, and content filters (see 8.2.3 Malicious software and hoaxes). The ITB also protects, implements, uses, tracks all use, and assists customers with the use of digital signatures, digital keys, digital certificates, secure Internet transactions, cryptographic tools, and other technical security controls. Managers of local communications, networks, and systems must ensure they document, implement, secure, maintain, oversee, and manage their local communications, networks, and systems consistent with enterprise standards.

8.3.2.3 Electronic commerce and E-government controls

Electronic commerce uses electronic mail, data interchange, on-line transactions, secure transactions, and other forms of automated communications to expedite business activity. E-government systems use Internet-based electronic commerce. Electronic commerce adds additional risk because it attaches EDD networks, computers, and communications directly to outside organizations and individuals. Managers responsible for electronic commerce must address internal and external security risks:

- a) Document and enforce their local information security controls based upon a thorough risk assessment; and,
- b) Ensure only HHSDC secure networks transmit confidential or sensitive information unless both the ISO and ITB provide advanced written approval.

8.4 Media handling and security

8.4.1 Media handling procedures

Managers must document, enforce, and at least annually review local information media handling procedures that define how to authorize and limit access to confidential and sensitive information, how to record that access, and how to handle and dispose of that media securely.

8.4.2 Management of removable computer media

Managers must protect removable media containing sensitive or confidential information with appropriate labeling, secure storage, and secure handling. Managers must protect removable media in compliance with manufacturer specifications and provide regular refreshing of magnetic media as magnetically stored information dissipates with use and over time (five to seven years).

8.4.3 Media and equipment disposal

Managers must ensure the complete erasure or destruction of sensitive or confidential information prior to disposal of media or equipment; e.g., paper, microfiche, diskettes, cassettes, disks, CDs, memory, laptops, personal digital assistants, servers, telephones, tape recorders, dictation machines, network appliances, etc. Although some media can be shredded or burned, many electronic devices and most media require special ITB or Department of General Services, Office of Machine Repair clearing. Managers must require this clearing to prevent commonly available utilities from recovering erased information from media and equipment.

9.0 ACCESS CONTROL

Access control policy statement:

The EDD will allow information interchange and access while protecting all information, operations, communications, and all underlying support technology, networks, systems, and documentation to acceptable levels of risk as defined by a risk analysis.

9.1 Business requirement for access control

The EDD Access Control Policy and External Access Control Policy set minimum standards and requirements that all individuals with access to EDD information assets must follow.

9.2 Individual access management

Managers must ensure their organizations document and use a registration and authentication process that only allows information owners to grant access rights, verifies access rights before allowing access to sensitive or confidential information, and revokes access when the need ends.

9.3 Individual responsibilities

All individuals must adhere to the Access Control Policy standards for ID and password construction, protection, and update frequency. Each must secure their work areas, terminals, personal computers, and other information processing equipment by following the EDD Clean Desk and Screen Saver policies.

9.4 Network access control

Managers must ensure those permitted information access comply with EDD network access control standards to avoid compromise of information, communications, or network security.

9.5 Operating system access control

Managers must document and enforce local controls to limit operating system access.

9.6 Application access control

9.6.1 Information access restriction

The EDD requires all applications to restrict access to sensitive and confidential information. The information owners must verify each individual requesting access has appropriate legal authority and a valid business need for access. Once those access rights are determined, they are stored within an application access system. That access system must require each individual to supply their unique customer identification (ID) and authenticate that is their ID (password, biometrics, etc.). Each application system must limit access to just the pre-authorized information.

9.6.2 Sensitive system isolation

Managers must identify, isolate, and protect every sensitive system within their work area. Sensitive systems include any application that processes confidential or sensitive information, processes or gathers information for financial or personnel transactions, oversees or monitors EDD communications, networks, or systems, or transmits like information to other agencies.

9.7 Monitoring access and use

The ITB appropriately secures, maintains, records, monitors, and reviews departmental network, communications, system access, and system use. Managers must provide equivalent documented protections for all local networks, communications, and systems to:

- a) Ensure systems that process confidential and sensitive information can maintain logs of history information to permit auditing, incident identification, event tracking, incident investigation, and incident resolution;

- b) Train and oversee individuals authorized access to ensure they follow local procedures;
- c) Keep each information system clock accurately synchronized to Pacific Time to provide an accurate link between system events and event logging; and,
- d) Provide ongoing review of communications, networks, systems, security services, and event history logs to detect any anomalous or suspicious events, then appropriately investigate, report, and address concerns or security incidents.

9.8 Mobile computing

Managers must conduct and document a risk assessment, then protect sensitive and confidential information assets accessed through mobile computing in accordance with that assessment. Mobile computing links terminals, workstations, portable computers, laptops, notebook computers, personal digital assistants, and other devices through modems, wireless connections, and other communications to permit remote access. Because these unsecured connections pose a gravely increased risk of unintentional disclosure, both the ISO and ITB must approve in advance the controls to protect each mobile computing request.

10.0 AUTOMATED SYSTEMS DEVELOPMENT AND MAINTENANCE

Development and maintenance policy statement:

The EDD utilizes a formal risk management process to develop and maintain the controls used to protect its communications, networks, and information systems throughout their life cycle from initial development, through changes, and into retirement.

Managers who oversee acquisition, development, and maintenance of communications, networks, and systems must comply with the same documentation, support, maintenance, oversight, and information security requirements that the ITB must follow. All new or significant upgrades to communications, networks, and systems must comply with Appendix I - Development and maintenance support. Significant upgrades include any project whose scope or cost requires an internal or external feasibility study report or changes existing information security protections. Managers must limit the number of persons with knowledge of and access to system development and maintenance technology and its documentation. Managers must limit access to development and maintenance technology to those with the appropriate technical skills, an authorized business need, and only for the duration of a specific business need.

11.0 CONTINUITY PLANNING MANAGEMENT

Continuity planning policy statement:

Each level of EDD operation will develop, document, maintain, test, exercise, and train staff in the continuity planning to protect clients, staff, and information assets during an emergency, and to provide an efficient prioritized restoration of business services following a disruption.

11.1 Aspects of continuity planning

Federal laws, State laws, and State administrative policy require formal business continuity planning for all levels of operation. The two aspects of continuity planning are emergency response (ER) and business resumption (BR) plans. The ER details the advance preparations and emergency actions to protect staff, clients, and information assets during and immediately following an emergency. The BR plans provide the detailed steps for efficient prioritized restoration of business services following a manageable disruption.

11.2 Business impact analysis

Each local office manager must regularly assess local risks and exposures then document that information in a business impact analysis.

11.3 Writing and implementing continuity plans

Each local office manager must prepare, implement, and forward their continuity plan to their branch that addresses the exposures identified in their business impact analysis. Each branch manager must ensure their branch consolidates their local continuity plans into a branch plan, and then forward by May 15th of each year the branch plan to the ISO. The ISO provides ER and BR templates and instruction:

- a) The ER defines the planning and preparations to survive an emergency or disaster:
 1. Procedures to acquire and maintain local emergency equipment, supplies, training, egress and assembly instructions, and communications to protect the health, safety, and comfort of clients and staff during and immediately after a business disruption;
 2. Procedures to contact and coordinate rescue efforts with local emergency and rescue personnel;
 3. Procedures and contact information to work through their chain of command, disaster coordination staff, emergency service providers, and the Operational Recovery Center (ORC) to keep the department informed of status and resource needs; and,
 4. Procedures to protect critical information assets and supplies from further damage during a disruption;
- b) The BR plan defines the planning, preparations, and detailed steps for an efficient prioritized resumption of business services:
 1. Prepare detailed BR plans with the steps, skills, resources, activation process, and actions to restore critical and essential business functions within 72 clock hours of a manageable business disruption;
 2. Prepare detailed BR plans with the steps, skills, resources, activation process, and actions for the timely restoration of all other business functions;
 3. Coordinate with the BOPSD to ensure availability of alternative facilities; and,
 4. Prepare and document any backup or maintenance plans or contracts coordinated through the BOPSD to address environmental or other utility failures; e.g., heating, air conditioning, filtration, or dehumidifier.

11.4 EDD Continuity Plan for Business (CPB)

The ISO uses the branch continuity plans to prepare the EDD continuity plan for business (CPB). The CPB provides the overall departmental ER and BR plan to define how EDD will respond to a national or widespread disaster. The CPB provides guidelines to help the Director and ISO in deciding when and at what level to activate the EDD primary or secondary ORC. It identifies critical business functions. It identifies the departmental chain of command and provides confidential emergency access information for the Directorate to contact and convene the division chiefs. It defines how EDD will contact and work with the Governor's Office, TOSU, the Highway Patrol, the Labor and Workforce Development Agency, agency data center, the Office of Emergency Services, law enforcement, and other emergency service providers. It defines how the ORC and Central Office support teams will coordinate resource deployment, coordinate resumption of critical business functions, and help restore business operations after a disruption. The ISO submits the Director approved CPB to control agencies including the Department of Finance each July 15.

11.5 Business continuity testing and maintenance

Each manager must document, maintain, and regularly test their continuity planing to ensure its ongoing currency, viability, and effectiveness. They must use scheduled and unscheduled reviews and at least annual scenario or simulation testing to thoroughly exercise and test all ER and BR components to protect against incorrect assumptions, oversights, or changes in personnel, business, equipment or technology. This testing must verify the currency and effectiveness of the advance ER and BR planning to ensure it includes sufficient detail, resources, and staff to effectively address a business disruption. This regular testing also helps educate new employees and keep existing staff aware of and proficient in their ER and BR skills. Each manager must record any deficiencies and maintain that testing record with their local continuity planning documentation available for auditing. Each local office manager must update their ER and BR continuity plans whenever a significant change in information assets or technology occurs or when testing finds the controls need improvement to address local deficiencies. Each local office manager must forward a copy of plan updates to their deputy director and any recommendations for departmental CPB changes to the ISO.

11.6 Emergency Response and Business Continuity Training

Each employee should become proficient in their ER and BR duties. Each manager must ensure their staff members receive initial and annual refresher training on their specific ER and BR responsibilities and duties, including how to:

- a) Help protect and care for staff and clients during and immediately after a disruption;
- b) Minimize damage to critical equipment, facilities, and supplies;
- c) Establish effective emergency communications; and,
- d) Facilitate a rapid prioritized recovery of critical then normal business services.

11.7 Business continuity planning activation

The office manager decides when to activate business continuity planning. Should a business disruption last 24-clock hours or longer, the office manager activates EDD's disaster communication structure by requesting assistance from their Area Division Disaster Coordinator. The Area Division Disaster Coordinator serves as the office communication and coordination hub. They forward requests for assistance and regular program status reports to the ISO and their Deputy Director who keeps the Director informed. In the event of a business disruption involving two or more offices, a regional disaster, a state-wide business disruption, or a national emergency or disaster, the directorate:

- a) Fully activates the primary or secondary ORC;
- b) Advises the Administration Branch and issues the appropriate disaster notifications through the ORC;
- c) Convenes program chiefs to serve as the Disaster Recovery Management Team (DRMT) to deploy department level resources to the impacted area via the CO support teams; and,
- d) Directs the ITB Deputy Director to restore communications, networks, and systems. The ITB contacts any needed service providers or expert consulting help. The ITB coordinates and resolves information technology emergency concerns while working through the ISO/ORC to keep senior management informed.

12.0 COMPLIANCE

Compliance policy statement:

The EDD will adhere to all Federal and State information security legal and administrative requirements for the development, acquisition, deployment, dissemination, maintenance, usage, and destruction of all information assets. Audits will regularly assess compliance.

12.1 Compliance with requirements

Managers must provide oversight to ensure all individuals authorized access to EDD information assets comply with legal and administrative requirements. The ISP provides the information that all EDD's users need to comply with applicable laws and regulations (see Appendix A – Statutory References). Individuals should consult with their manager when in doubt regarding existing information security policy, legal requirements, or contractual obligations. Managers should consult with the EDD Legal Office for legal clarification or assistance, and with the ISO for information security clarification or assistance.

12.1.1 Copyright and Intellectual property rights

Managers must ensure all individuals within their areas comply with copyright laws and the ITB maintained Software Copyright Policy to appropriately protect proprietary information. Managers must oversee software inventory and distribution to ensure all individuals in their areas only run legally licensed copies of software authorized for their specific computers. Beginning January 31, 2004, and ongoing, EDD must submit to the Department of Finance an annual certification along with the summary of updated inventories conducted by the department as part of its ongoing software management practices. This certification must also identify the individual responsible for ensuring department compliance with the California Software Management Policy.

12.1.2 Security of confidential and sensitive information

Each individual authorized access to confidential and sensitive information must secure that information and handle any requests for the release of such information in accordance with all legal and administrative requirements for access.

12.1.3 Misuse of information processing technology

The law requires EDD managers to monitor, report, and appropriately prosecute any misuse of information processing technology. Each manager must inform those they oversee of proper information usage and potential repercussions for misuse.

12.1.4 Regulation of cryptographic controls

Managers and the ITB must provide monitoring and oversight of cryptographic controls to ensure staff do not illegally share or export certain controls, and ensure that staff do not use cryptographic controls to mask or hide inappropriate or criminal activities.

12.1.5 Collection of evidence

When anyone recognizes a potential information security exposure they must immediately contact their management. Managers who decide to conduct an investigation must work closely with the Investigation Division, Internal Affairs Unit to avoid potential legal problems. The Internal Affairs Unit provides instruction to appropriately gather, preserve, and protect any evidence in accordance with legal rules of evidence requirements. Managers involved with systems development and maintenance must verify with the Investigation Division and the ITB to ensure the quality, completeness, and legal admissibility of any evidence collected, including audit and activity logs.

12.2 Reviews of security policy and technical compliance

12.2.1 Compliance with security policy

Unless exempted by the Chief Deputy Director, managers must document and verify through at least annual testing, information security reviews, and ongoing monitoring to ensure their staff, areas, and information assets comply with the ISP, technical security requirements, and any additional required local information security requirements. Auditors will inspect these compliance efforts and documentation.

12.2.2 Technical compliance checking

The ITB must provide regular written security reviews and provide appropriate ongoing checking, monitoring, and auditing of all Departmental communications, systems, networks, applications, hardware, software, other information assets, and ongoing usage to ensure compliance with EDD information security requirements. Managers who oversee local systems must conduct and document similar ongoing formal regular review, testing, and monitoring. Authorized persons other than those who provide ongoing system maintenance or operations must oversee these reviews to verify information security technical compliance.

12.3 System audit considerations

12.3.1 System audit controls

Managers must coordinate all audits through the Audit and Evaluation Division (A&ED). A&ED oversees and controls all auditor access and the use of auditing tools to ensure the effectiveness of audits while minimizing any disruption to operational systems and production activities during the audit process.

12.3.2 Protection of system audit tools

Unauthorized individuals and malicious software will frequently target system audit tools to take advantage of their ability to bypass normal security controls to provide unauthorized access. The EDD carefully limits audit tool access, prevents audit tool compromise, and safeguards audit tool integrity by keeping such tools closely monitored and separated from development and operational systems. When stored in tape libraries, servers, or other employee accessible areas, these tools require encryption or password protection. Managers must preclude storing these audit tools on desktops, laptops, shared or personal network libraries, without the written consent of the ITB Deputy Director and the ISO Chief.

12.4 External auditor access

Only deputy directors and above may authorize external auditor access, and only A&ED may coordinate external audits. Any individual receiving an external auditor access request must immediately notify their management who will notify the A&ED Chief. The A&ED works closely with the deputy directors to coordinate auditing functions to minimize disruption of business services. The A&ED will obtain confidentiality statements from external auditors in compliance with disclosure requirements before allowing access to EDD's systems or confidential and sensitive information.

APPENDICES

APPENDIX A - STATUTORY AUTHORITY

These statutes, regulations, and administrative policies provide the primary legal authority for the ISP and govern EDD information security and disclosure.

California state laws

The California State Constitution article 1

Regulates classification and dissemination of information and guarantees individuals' right to privacy.

Government Code section 6250- et seq. (The California Public Records Act)

The PRA provides that all public records maintained by the Department be made open to the public for inspection during regular office hours and that copies of the records be provided persons requesting them within reasonable time periods. The PRA exempts from disclosure certain types of Department records, including records pertaining to pending litigation, personnel, medical, or similar federal law. As a general rule, records the Department may disclose under the PRA are those which are non-personal in nature. The Act is enforceable through a civil court action.

Government Code section 11019.9

Requires all state agencies enact and maintain a permanent privacy policy in adherence with the Information Practices Act of 1977. Requires each agency assign a Privacy Officer to ensure compliance.

Government Code sections 11773 through 11775

Mandates each state agency to develop a Disaster Recovery Plan with respect to information technology and to file a copy of its plan with its control agency annually.

Government Code sections 14740-14770 (The State Records Management Act)

Provides for the application of management methods to the creation, utilization, maintenance, retention, preservation, and disposal of state records, including determination of records essential to the continuation of State government in the event of a major disaster. (SAM sections 1601 through 1699 contain administrative regulations in support of the Records Management Act.)

Labor Code section 6401.7

Mandates all employers have work site safety plans.

The California Unemployment Insurance Code (CUIC)

Provides that information obtained by the EDD, in the course of its administration of the CUIC, which identifies a particular individual or business entity is confidential. It contains several provisions restricting the use and disclosure of information, including Sections 1094, 1095, 2111, and 2714.

The term "confidential" as utilized by these provisions, means that the privacy of such information is to be maintained. Disclosure of confidential information can only occur under specific circumstances. Confidential information cannot be used as evidence in any proceeding unless it is one that arises under the provisions of the Code. A violation of the confidentiality provision is punishable as a misdemeanor and cause for adverse action against an employee.

Civil Code sections 1798 et seq. (Information Practices Act of 1977)

Protects the individuals' right to privacy. Places specific requirements on state agencies for the collection, use, maintenance, and dissemination of information relating to individuals. Provides for the disclosure of all personal information maintained by public agencies. Confidential information can only be released to the data subject, to a third party authorized by the data subject, or a third party, on a need-to-know basis, that is specifically required by state or federal law to use this information for the administration of their statutory programs.

Penal Code section 502 (Comprehensive Computer Data Access and Fraud Act)

Expands the degree of protection afforded to individuals, businesses and governmental agencies from tampering, interference, damage and unauthorized access to lawfully created computer data and computer systems. It allows for civil action against any person convicted of violating the criminal provisions for compensatory damages.

California state administrative policies

State Administrative Manual (SAM)

The SAM requires development and implementation of specific policies and procedures for the protection of information assets and to ensure the continuation of business operations. Additionally, the SAM provides specific administrative regulations in support of the Records Management Act.

EDD Administrative Manual No. 10, the Information Practices Handbook (IPH)

State laws place specific requirements on the EDD with respect to its collection, use, maintenance, and dissemination of information relating to individuals. These requirements are set forth in the California Public Records Act, the Information Practices Act, the State Records Management Act, and various provisions of the Unemployment Insurance Code.

The Information Practices Handbook (IPH) helps employees understand the laws affecting the Department's information practices. The IPH also provides specific procedures and rules of conduct for employees regarding the use and disclosure of information collected by the Department in the administration of its various programs.

Federal laws

The Social Security Act 42 U.S.C.A. Chapter 7, Section 503

Provides grants to states which have an unemployment compensation law, approved by the Secretary of Labor under the Federal Unemployment Tax Act, for the administration of the Federal/State Unemployment Compensation program.

The Comprehensive Computer Data Access and Fraud Act 5 U.S.C.A., Section 501

The Economics Espionage Act of 1996 defines the term "proprietary economic information" if reasonable measures have been taken to keep such information confidential, and if the information derives independent economic value from not being generally known to or accessible by the public.

The Computer Fraud and Abuse Act 18 U.S.C.A., Section 1030

Bars trafficking in passwords. Bars transmitting code that damages or changes the use of a computer system, computer services, a network, or data.

The Electronic Communications Privacy Act 18 U.S.C.A., Section 2510 et seq.

Extends protections for telephone privacy to computer mediated electronic transmissions.

The Federal Privacy Act (FPA) 5 U.S.C.A. (section 552a)

The FPA relates primarily to federal agency records. It requires the maintenance of systems of records and provides for restrictive disclosure of federal records maintained on individuals. These statutes are generally only applicable to federal agencies.

The Freedom of Information Act (FOIA) 5 U.S.C.A. (section 552)

Governs access to records of federal agencies and can be used by the EDD to obtain records from the federal government. It does not govern access to State records of State agencies.

The Federal Government Information Security Reform Act (GISRA)

Regulates automated information security and access policies, practices and protections.

Internal Revenue and Taxation Code

Regulates the use of Internal Revenue Service information by the EDD.

Office of Management and Budget Circular A130 (OMB-A130)

Regulates automated information security and access policies, practices and protections.

APPENDIX B - INTERNATIONAL STANDARD - 17799 SUMMARY

1. Security Policy

Top management should set a clear direction and demonstrate their support for and commitment to information security through the issuance of an information security policy across the organization.

2. Security Organization

The objective of the information security infrastructure is to manage information security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Responsibilities for the protection of individual assets and for carrying out specific security processes should be explicitly defined.

3. Asset Classification and Control

The objective of assigning accountability for information assets is to maintain appropriate protection of organizational assets. All major information assets should be accounted for and have a nominated owner. Inventories should be maintained of all major information assets.

4. Personnel Security

The objective of personnel security is to reduce the risks of human error, theft, fraud, or misuse of facilities. Security should be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during an individual's employment.

5. Physical and Environmental Security

The objective of physical and environmental security is to prevent unauthorized access, damage and interference to IT services. IT facilities supporting critical or sensitive business activities should be physically protected from security threats and environmental hazards.

6. Communications and Operations Management

The objective of network and data center management controls is to ensure the correct and secure operation of computer and network facilities. Responsibilities and procedures for the management and operation of all computers and networks should be established.

7. Access Control

Access to computer services and data should be controlled on the basis of business requirements. Formal procedures should control allocation of access rights to IT services including computer systems, network services, applications, and data. To detect unauthorized users or activities, systems should be monitored.

8. Systems Development and Maintenance

Security requirements should be identified and agreed to prior to the development of IT systems to ensure that security is built into IT systems.

9. Business Continuity Management

Business continuity plans should be available to protect critical business processes from the effects of major failures or disasters.

10. Compliance

The objective of security monitoring is to ensure compliance with organizational security policies and standards. The security of IT systems should be regularly reviewed.

APPENDIX C - INFORMATION SECURITY POLICIES

The EDD's information security policies help make inter-connectivity between work groups possible, keep overhead and maintenance manageable, and help describe items to be procured. Although technical standards change frequently, they are mandatory as long as they are in effect. Deviation requires approval, in writing, from the Deputy Director, ITB, and the ISO. Technical Standards, Procedures and Guidelines are omitted from this document, but will be linked with the ISP as they are developed. Refer to the following documents for information on existing Technical Standards, Procedures, and Guidelines.

<u>Title</u>	<u>Document Type</u>	<u># or Date</u>
Business Driven Architecture Policy	IT Circular	00-03B
Cellular Telephone Policy	IT Circular	01-01 C
EDD Administrative Manual	Management Handbook	NA
Electronic Mail - Procedures for Use of Electronic Mail for Event and Activity Notification	Executive Notice	97-08 C
External Customer Access Policy (see Inside EDD references)	ITB Policy	12/21/95
Facsimile (Fax) Policy	Administrative Circular	97-02 C
Guidelines to Maintain Security of Laptop Computers	Executive Notice	93-04 B
Information Practices Handbook	EDD Administrative Manual	Chpt 10
Internet Policy	IT Circular	99-05 C
Procedures for Completing EDD Appointment/Separation Clearance Checklist	Executive Notice	91-5 B
Procedures for Completing EDD's Confidentiality Statement (DE 7410 and DE 9000)	Executive Notice	91-6 B
Procedures for Reporting of Security Incidents Involving the Department's Information Assets (DE 7413)	Executive Notice	02-01 C
Security Awareness Training Program	Executive Notice	96-15 GE
Telephone Toll Fraud Policy	Executive Notice	96-06 C
Voice Mail Policy	IT Circular	01-04 C
Workgroup Computing Policy (see Inside EDD references)	IT Circular	00-03 B
Software Copyright Policy	IT Circular	02-02 B
User Identification (ID) and Passwords	IT Circular	99-03 C

APPENDIX D - SUMMARY OF INFORMATION SECURITY RESPONSIBILITIES

Individuals with access

Each individual authorized access to EDD information assets must:

- a) Become and stay familiar with the EDD and local information security policies and good information security business practices; and,
- b) Protect and secure the information assets they access.

EDD employee

Each EDD employee authorized access to EDD information assets must:

- a) Attend initial and ongoing annual information security training;
- b) Carry out their duties to help preserve business continuity;
- c) Prevent, detect, report, and minimize compromise of information assets or secure areas;
- d) Report all identified and suspected information security incidents (see section 6.3);
- e) Protect the health and safety of staff and customers during and immediately after a disruption; and,
- f) Become proficient at their duties for a rapid prioritized restoration of business services following a disruption.

Managers and supervisors

Each manager and supervisor must:

- a) Oversee information security for their assigned staff, areas, and information assets;
- b) Maintain a current inventory of locally used software packages that can be audited, and forward that inventory by October 15th each year to their branch management;
- c) Prepare staff with the required initial and annual refresher information security training;
- d) Provide oversight to ensure appropriate use of State owned hardware, software, networks, and other information assets;
- e) Ensure proper authorized access, modification, and dissemination of sensitive and confidential information;
- f) Prepare their office with the emergency supplies, plans, and training needed to protect the health and safety of staff and customers during and immediately following a disruption; and,
- g) Prepare their office with the planning, training, and preparation to ensure the rapid prioritized recovery of business services following a disruption.

Branch management

- a) Consolidate all branch office critical applications, emergency response, and business resumption continuity planning along with branch planning into a branch plan then forward that branch continuity planning to the ISO by May 15th of each year; and,
- b) Consolidate all branch office software inventories in accordance with SAM requirements into a branch inventory and submit that combined inventory to the ITB by November 15th of each year.

Information Technology Branch (ITB)

The ITB Chief must:

- a) Oversee the ITB and all EDD system administrators;
- b) Provide EDD with specialized information security oversight, support, expert technical guidance, and physical security for centralized information assets;
- c) Monitor ongoing operations, systems, and networks to ensure security and provide early detection of security risks, exposures, and incidents;
- d) Coordinate and work closely with the ISO, the HHSDC technical staff, and information security contractors to keep the department and systems administrators current with information security technical support; e.g., virus warnings, system updates, and software patches;
- e) Provide a ready source of expert guidance and investigative resources at the earliest possible stage following a suspected information security incident;
- f) Advise on, lead, or conduct security incident technical investigations as directed by ITB senior management, the ISO, Investigation Division, Legal Office, or the Directorate;
- g) Approve and test new system designs for security and recovery capabilities;
- h) Oversee and protect the EDD network;
- i) Provide technical information security policies, oversight, and services; and,
- j) Maintain an inventory of central EDD software as required by the state administrative manual and combine that inventory with branch software inventories then forward the results to the Department of Finance prior to January 31 each year.

Information Security Officer (ISO)

The Information Security Officer must:

- a) Manage the Information Security Office (ISO);
- b) Coordinate the implementation of information security controls;
- c) Oversee the EDD information security program;
- d) Develop and maintain the ISP;
- e) Develop and maintain other supportive administrative information security policies;
- f) Require and approve supportive information security technical policies;
- g) Address, resolve, and document security incidents and provide required control agency incident reporting;
- h) Provide the ISP for required annual control agency review; and,
- i) Submit departmental Business Continuity Plan for required control agency review.

Business Operations and Planning Support Division (BOPSD)

The BOPSD must:

- a) Coordinate with program staff to ensure appropriate information and environmental security in EDD central, remote, and partner sites; and,
- b) Validate all new contracts contain appropriate information security.

Audit and Evaluation Division (A&ED)

The A&ED must:

- a) Conduct regular reviews and/or internal audits to ensure compliance with enterprise security policies, standards, procedures, and guidelines;
- b) Oversee external audits to protect information and comply with legal requirements; and,
- c) Oversee the use of auditing and monitoring tools.

Investigation Division, Internal Affairs Unit

The Investigation Division, Internal Affairs Unit must:

- a) Provide instruction to appropriately gather, preserve, and protect any evidence;
- b) Oversee the evidence gathering process; and,
- c) Provide required internal information security audits.

Human Resources Services Division (HRSD)

The HRSD must:

- a) Coordinate information security human resources activities; and,
- b) Ensure conformance with union contracts and State policy.

APPENDIX E - EVIDENCE OF COMPLIANCE

Policy compliance requires maintaining the following documentation available for auditing:

Each local office:

- a) A local risk assessment that identifies secure areas; all local information assets with clear access rules, rights, and authorities for each asset; risks for each asset and selects any required additional local controls; and documents those additional controls in a local information security policy;
- b) Local information security training materials, requirements, and completion records;
- c) Local ER and BR continuity plans to respond to security incidents and malfunctions;
- d) Documented logs, transmittals, and other records used to verify information security and the accurate timely delivery of services; and,
- e) Documented results from testing information security policies and business continuity planning.

Each branch:

- a) Inventory of branch information assets with individual access management controls for each program;
- b) Job definitions that include individual information security requirements;
- c) Initial and ongoing individual screening results;
- d) External controls for auditor access;
- e) Branch process for responding to and reporting security incidents and malfunctions;
- f) Current branch ER and BR continuity planning that identifies local critical business functions; and,
- g) Documented regular assessment and testing results that verify local office and branch effectiveness in implementing the ISP, local information security policy, and continuity planning.

All developers and maintainers:

of EDD information systems, communications, or networks including the ITB must develop and maintain documented procedures, responsibilities, and acceptance controls for systems, applications, and communications:

- a) Security controls for system and network development, testing, support, and monitoring;
- b) Cryptographic, authentication controls, and management process;
- c) Security of application, system, and network access and tracking logs;
- d) Security controls for maintaining programs, files, databases, and documentation;
- e) Controls for exchanges of information and software; and,
- f) System housekeeping function controls (backup logging, etc.).

Information Security Office:

- a) The ISP and supportive detailed information security and access control policies;
- b) The departmental continuity plan for business; and,
- c) The EDD CPB.

Business Operations Planning and Support Division (BOPSD):

- a) Full inventory with contacts for all EDD and partner sites;
- b) Physical, environmental, and emergency security requirements; and,
- c) Process to validate information security in contract approval process.

Audit and Evaluation Division (A&ED):

- a) Review of security policy;
- b) Review of technical compliance; and,
- c) Documented results of required audits.

Human Resources Support Division:

- a) Maintain individual information security training records;
- b) Procedures for screening employees and contract staff; and,
- c) Procedures for providing individual oversight.

APPENDIX F - EDD MAJOR SYSTEMS

Major Systems

Information Owner

Abstract System	Director's Office
Disability Insurance (DI) information and Single Client Data Base (SCDB) system	Disability Insurance Branch
Human Resources Systems	Human Resource Services Division
Cal JOBS System	Job Services Branch
ES 202 and other labor market information	Labor Market Information Division
Base Wage Database System	Tax Branch
Independent Contractor Reporting System (ICRS)	Tax Branch
Internet Filing (IFILE)	Tax Branch
Internet Independent Contractor Reporting System (IICR)	Tax Branch
Internet New Employee Registry (INER)	Tax Branch
New Employee Registry System (NER)	Tax Branch
Tax Accounting System (TAS)	Tax Branch
Unemployment Insurance (UI) information and SCDB system	Unemployment Insurance Branch
Job Training Automation System	Workforce Development Branch

APPENDIX G - INFORMATION LABELING AND HANDLING

Information Labeling	<p>Managers, supervisors, and system administrators must ensure appropriate labeling of all confidential and sensitive information. This includes labels on printed reports, screen displays, facsimile (fax), and other physically viewable information. Electronic and magnetic media; e.g., tapes, diskettes, storage discs, cassettes, and cassette/laser disks (CDs), used to transport confidential or sensitive information must also contain appropriate external labels. Automated data stores do not need labeling, at the field, or any other level, stored in the automated file itself. The SCDB, TAS, and Base Wage Databases, and other major EDD files are confidential. Data files extracted from these databases are treated separately and labeled according to the data contained on the extract.</p>
Information Sharing	<p>State and federal laws recognize EDD's information as a public resource that must be protected from inappropriate disclosure. EDD policy complies with legal requirements by limiting release of information or records in accordance with their classification.</p> <p>Individuals must only share sensitive and confidential information with others with a legal right for access and a valid business need-to-know. Individuals must only share sensitive or confidential information in secure areas or by using ITB and ISO approved communications; e.g., the EDD internal network, the United States Postal Service, and couriers with appropriate licensing and bonding. Managers must provide advance written approval before an individual removes any confidential or sensitive information from EDD premises.</p> <p>Individuals must not use unsecured communications to share or discuss any confidential or sensitive information; e.g., fax, electronic mail, the Internet, public networks, voice mail, mobile/cell phone, and answering machines. They must not use unsecured electronic devices to store, process, print, or transmit confidential or sensitive information; e.g., memory or drives on workstations, personal computers, laptops, handheld computers, or personal digital assistants. Individuals must not share confidential or sensitive information in public places, public meetings, seminars, lectures, or other presentations.</p>
Confidential Information Access	<p>Federal and state laws authorize an individual or their authorized agents to access, inspect, and disclose confidential information and records specific to that individual. These authorizations may be written or verbal but the requester's identity must be verified before releasing any confidential information.</p> <p>The EDD releases confidential information to other governmental agencies when specifically required by law. These disclosures take place under the terms and conditions of reimbursable confidentiality agreements.</p> <p>Systems that allow access to confidential information must comply with the EDD Access Policy and Privacy Policy requirements. Access must secure confidential information by ensuring user identification and authentication, audit trails, and system access parameters to limit access only to the information required by the requester's business function, and as authorized by law.</p>
Sensitive Information Access	<p>Federal laws, state laws, and administrative policy require release of sensitive information when requested by authorized governmental agencies. These laws and policies preclude individuals and organizations granted access to sensitive information to release that information to other parties. Unless exempted by law, before releasing information to a requesting agency, that agency must complete appropriate non-disclosure agreements.</p>

Public Information Access	Upon a request for public information, the Public Records Act requires EDD to provide that information in no more than 14 days. Department practice is to provide requested information within 10 days. It must be provided in an easy to use and understand format. Released information must not contain any confidential information, sensitive information, or encrypted data. All release of Information for research purposes must comply with the EDD <u>Researcher's Policy</u> .
Information Storage	Managers must document any special information storage or retention needs in accordance with program and legal requirements. Only computers and servers maintained in a secured environment may store and process confidential and sensitive electronic information. Individuals may not use personal computers, laptops, desktops, personal digital assistants (PDAs); e.g., palmtops and electronic planners, wireless devices, or personal computer media to store confidential or sensitive information without a written approval from the information owner and without implementing appropriate security controls, preferably encrypting confidential and sensitive information. Managers must ensure regular refreshing of stored media onto current technology to ensure normal magnetic degradation and usage does not result in information loss.
Access Notification	Prior to granting access to confidential and sensitive information, automated systems must provide a notification or warning banner at logon that says unauthorized access is prohibited by law (see Appendix J – Sample messages).
Client Confidential Information Release Notice	Prior to allowing a client to authorize the release of their own confidential information for public viewing and use, that client must be advised with an information release notice that explains if they provide that authorization, they forfeit their right to privacy (see Appendix J – Sample messages).
Information Integrity	Only authorized individuals may view, add, change, update, or delete information and must do so through an authenticated and monitored process.
System Design	Each new system or significant change to an existing system must incorporate information security and business continuity as an integral part of the design. The design documents must specify sufficient security to appropriately protect all confidential and sensitive information and provide all of the needed backup materials and resources to rapidly resume full service delivery.
Process Monitoring	Appropriate manual and automated means must monitor and log all information access and processing to help prevent and detect unauthorized information inspection, access, use, modification, and destruction.
Audit Trails	All systems must include audit trail facilities to permit recording every access to confidential and sensitive information.

APPENDIX H - INFORMATION SECURITY TRAINING REQUIREMENTS

At a minimum, security awareness training, and education must address:

- a) An overview of the ISP and local security policies with instruction on how to find relevant detailed security requirements and forms;
- b) A definition of how to classify, label, and handle information to keep all confidential and sensitive information secure;
- c) The requirement to use information assets securely and only for EDD business purposes;
- d) A clear understanding of the potential severity and repercussions of any information security incident to both the Department and the responsible individual;
- e) Specific additional program and local requirements for information security, emergency response, and business resumption;
- f) The requirement to immediately report any information security incident or suspected incident to their immediate supervisor or manager;
- g) Knowledge of their emergency response and business resumption duties and responsibilities defined in their local emergency response and business resumption planning; and,
- h) Good security practices as only diligent, knowledgeable individuals can prevent information security incidents from happening and mitigate damage by early incident detection:
 1. Depending upon what you feel is safe, either report or challenge any unescorted individuals and anyone not wearing a valid identification badge in secure areas;
 2. The need to never discuss sensitive or confidential information in a public place, open office, or on a telephone, cell phone, or fax that would allow information to be overheard, intercepted, or inappropriately recorded;
 3. The need to not discuss organizational operating systems, servers, policies, procedures, and/or other security programs with anyone who does not have a "need to know";
 4. Good computer security awareness policies, practices, and standards, including using password logon protection, using automatic processes to log-off or initiate a screen saver after no more than ten minutes of non-activity that require a password to log back on, using strong password selection, and using regular password modification. Individuals should never write down, hide, or give their computer IDs and passwords to anyone;
 5. Good answering machine and voice mail practices including never leaving messages containing sensitive or confidential information and never listening to messages on a speaker phone where an unauthorized individual might overhear;
 6. Good fax practices including always double checking to ensure sending to the right person, securing fax systems that store confidential numbers or other sensitive information, and securing fax systems that do bulk transmissions; and,
 7. Good electrical power management practices as uncoordinated power loss can severely damage information technology equipment and lose or damage information;
 8. The proper use and care of information technology equipment, programs, software, and media.

APPENDIX I - DEVELOPMENT AND MAINTENANCE SUPPORT

This appendix provides the information security and documentation requirements that EDD organizations and staff must follow when designing, developing, configuring, installing, running, maintaining, and managing communications, networks, and information systems. These requirements apply to all new development, to all changes whose scope or cost requires a feasibility study report, and whenever a change impacts existing EDD information security measures, e.g., firewall, access control, security service, etc. Project managers should ensure all their projects comply with these requirements, but must ensure their projects comply with these requirements whenever their projects deal with confidential or sensitive information or if their project supports any critical business function.

I.1 Planning documentation

Planning documents identify project scope, objectives, requirements, resources, costs, and timing so management can make informed approval decisions for new projects and significant upgrades. Cost, time, and resources often preclude retroactively adding information security. Before project initiation the ISO and the ITB must review and approve planning documentation to ensure it requires building in information security and provides ample resources to maintain information security for the life of the project. Planning documents include all Feasibility Study Reports (FSRs), Request for Proposals (RFPs), Invitations to Partner (ITPs), Requests for Qualifications (RFQs), Invitations for Bids (IFBs), vendor proposals, the Workgroup Computing Policy and Guidelines, and vendor contracts.

I.2 General design documentation

The general design documentation sets the general rules and requirements associated with developing and maintaining communications, information systems, and networks. The ITB as responsible for central EDD communications, information systems, and networks, maintains appropriate information security controls in the ITB Software Engineering Project Life Cycle to set a consistent rigorous approach to project implementation and maintenance. Project managers must follow this or an ITB approved equivalent approach. At a minimum the project manager must ensure the general design documentation includes both implementation and operational plans that incorporate the needed information security controls. That documentation must include a thorough test plan to verify the operating procedures and implementation incorporate those controls. It must include any special considerations for ongoing maintenance and monitoring to maintain ample security and capacity. Before starting development, the ISO and ITB must approve the general design documentation.

I.3 Detail design documentation

Whether developed by EDD staff or through a contractor, the detail design documentation must follow a systematic approach that meets the requirements of, and preferably follows the format of the ITB Software Engineering Project Life Cycle. This approach inventories assets and potential risks, analyzes potential impact, then develops and documents the most cost-effective information security controls to eliminate or mitigate those risks. Before starting development, the ISO and ITB must approve the detail design documentation.

I.3.1 Risk analysis and impact assessment

Each project must include a risk analysis and impact assessment. The risk analysis identifies and documents all critical and essential business functions and each information asset. It identifies and documents each potential risk and the likelihood of each risk occurring. Some of the risks evaluated include natural or man-made disruption or disaster; e.g., fire, flood, unauthorized entry, earthquake, civil unrest, explosion, terrorist attack, electrical power problems,

noise, fumes, water leakage, disruptions from neighboring premises, etc. It identifies and documents the likelihood for each identified risk or exposure occurring and assesses the potential worst case operational and financial impact from each risk on both information assets and business functions.

1.3.2 Risk mitigation plan

Each project must include a risk mitigation plan that selects and documents the most appropriate and cost effective controls, resources, technology, and alternatives to avoid or minimize the damages from the exposures identified in the risk analysis and impact assessment. Risk mitigation plans should follow the formats of the ITB System Requirements Specification and ITB Architectural Description. At a minimum this documentation must address the protection information assets with appropriate instruction for backup and recovery, and; e.g., workstations, laptops, personal digital assistants, desktop computers, and server computers.

- a) The verification, validation and testing process to ensure proper operation and that the system implementation does not adversely impact other information assets or existing controls;
- b) The requirements to keep these controls effective and current;
- c) The required access controls to ensure only authorized people may access documentation, development tools, programs, applications, processes, authorization processes, data structures, and other information; and,
- d) The requirements for the secure storage of this documentation.

1.3.3 Implementation plan

Each project must include an implementation plan that defines the information security checks, balances, controls, protections, and training needed for development, testing, operations, maintenance, oversight, monitoring, and system retirement to ensure information security for the life of the system:

- a) Preclude unauthorized inspection, access, use, modification, or destruction;
- b) Limit access rights to applications, services, networks, and information (authorization);
- c) Validate user identity before allowing access (authentication);
- d) Ensure processing errors and deliberate acts do not corrupt information or disrupt services;
- e) Provide security monitoring, error recovery logging, tracking, restart, backup, and contingency plans for alternative processing;
- f) Utilize any needed digital signatures and encryption to protect sensitive information, confidential information, data stores, and transmissions;
- g) Use non-repudiation services to validate the integrity, accuracy, and completion of activity, transactions, and data transmissions;
- h) Ensure programs, modules, and events run in the correct order and resume in the proper order after a disruption;
- i) Verify the ongoing integrity of information with downstream edits; and,
- j) Protect against availability disruptions caused by insufficient capacity or operational inefficiencies; e.g., disk fragmentation, insufficient bandwidth, improper configurations, excessive noise, etc.

1.3.4 Operating procedures

Each project must include written operating procedures with detailed information security requirements. This includes documentation of local start up, shut down, restart, error recovery, job scheduling, timing, processing, coordinating with other jobs, and back up. It includes the processes for managing any special forms, checks, or other confidential or sensitive processing. It includes housekeeping procedures; e.g., maintenance, mail handling, computer room upkeep,

testing, and safety. It also includes access control, security logging, process controls, monitoring, audit review requirements, and emergency contacts with notification procedures.

1.3.5 Test plan

Each project must include a written test plan and a log that documents all new development, significant operational changes, and testing results. Managers must maintain the plan and log available for auditing. The test plan must:

- a) Maintain a record of who may authorize each level of development or change and ensure only authorized individuals do that work;
- b) Ensure all changes are communicated to all relevant persons and thoroughly analyzed for their potential impact on all communications, networks, systems, hardware, and operations;
- c) Document anticipated test results and obtain formal customer approval for detailed proposals or changes before work commences; and,
- d) Document the steps for a prioritized recovery of business services with rollback procedures to abort and recover from a testing failure or unsuccessful changes.

1.3.6 Operational change control plan

Each project must include an operational change control plan that complies with and preferably follows the format of the ITB Configuration Management Plan. This plan sets the requirements so subsequent operational changes or maintenance activities do not disrupt business functions, impact functionality, cause information security incidents, or compromise existing information assets or controls. As part of the operational change control plan, each project must include a development and maintenance log that documents development and change activities. Both the ITB and ISO must provide advance written approval of that plan before project implementation may begin. Managers must maintain the development and maintenance log available for auditing.

1.3.7 Capacity planning and monitoring plan

Each project must include capacity planning and a monitoring plan that sets the requirements for ongoing oversight, monitoring, and review to ensure ample ongoing capacity.

1.3.1 System and information backup

The ITB and HHSDC protect EDD central systems through regular backup and testing. As required by the Unemployment Insurance Code for the major systems, ITB maintains four full sets of current backup information with two sets stored locally and two stored at a secure off-site location. BOPSD ensures that off-site storage locations comply with State requirements prior to contracting for secure data storage services. HHSDC also maintains contracts with third parties to ensure the rapid availability of alternate information technology resources to resume business functions following a disruption. Managers must provide appropriate equivalent protections for locally developed systems. They must ensure their backup planning includes all of the instructions, system software, applications software, hardware setups, files, databases, encryption keys, and anything else needed to rapidly resume operations. Managers must exercise their backup procedures at least semi annually and report any testing failures to the ISO as security incidents. Documented backup procedures and test results must remain available for auditing.

1.3.2 Operator, event, transaction, network, and system logs

Managers must meet mandated auditing and tracking requirements by maintaining appropriate logs to assist in problem diagnosis, corrective action, emergency repairs, event reconstruction, and capacity planning. At a minimum these controls must include:

- a) A written log that records all production system changes, authorizations for those changes, system releases, system tests, system monitoring, and audits;
- b) Facilities to capture and secure detailed operator, event, transaction, network, and system logs that record all relevant status information at the time of a disruption; and,
- c) Management activated facilities that can log all transaction and network activity to help diagnose problems and to ensure the completeness of repairs.

I.3.3 Data validation

All new application systems must thoroughly validate all input and output data. Each system must verify entry for valid characters, acceptable values, completion of all required fields, consistency of entries (totals balance), and plausibility of entries; e.g., ensuring check amount consistency of from month to month noting undue variances. Web applications must further validate client and server input to avoid intentional errors used for system penetration and exploitation. Entry edits do not address subsequent tampering, so EDD requires documented procedures, responsibilities, training, system checks, and appropriate monitoring to validate output data:

- a) Provide automated checks to verify data reasonableness;
- b) Provide reconciliation control counts to ensure processing of all data;
- c) Provide sufficient information for a reader or subsequent processing system to determine data accuracy, completeness, volumes, precision, classification, and labeling;
- d) Provide procedures for responding to validation test problems; and,
- e) Define the responsibilities for all personnel involved in the data output process.

Include additional checks and controls for on-line systems:

- a) Ensure the accuracy of out-bound content; e.g. Web pages, screens, and reports; and,
- b) Validate transactions on both client and server side for web applications;

Include additional checks and controls for batch systems to:

- a) Reconcile record counts after transaction updates;
- b) Verify opening and prior counts and balances to ensure consistency from run-to-run and after updating;
- c) Verify system-generated data;
- d) Utilize appropriate hash totals of records and files;
- e) Appropriately protect spooled data awaiting output; and,
- f) Verify the correct timing and run order for application programs.

I.4 Development and maintenance controls

Managers must ensure the secure development and maintenance of operational software and the security of all related files, test data, and documentation that enable, document, or permit testing of EDD business functions, communications, systems, networks, and applications.

Managers must limit and monitor vendor, contractor, and supplier physical and logical access to just that period required for operational software support and revoke access immediately after completion.

I.4.1 System Testing

Each project must follow its test plan and document the testing results. Managers must maintain a log of all testing activity and results, then keep that log available for auditing. The testing must:

- a) Thoroughly test to verify and document that all work done meets design requirements and anticipated results;

- b) Maintain version control for all updates and ensure production implementation adheres to version control standards;
- c) Verify that the work performed does not adversely impact the operation or security of other communications, networks, or systems before incorporating them into production; and,
- d) Ensure updating of documentation for each change and appropriately archive prior versions.

1.4.1 Protection of system test data

Managers must protect and control all system, application, and test data. Use of operational data or databases containing confidential and sensitive information for testing requires keeping that test data secure, safe, and appropriately separated from production environments.

1.4.2 Separation of development and production systems

Managers involved in development, maintenance, testing, or production operations must provide clear separation and oversight to keep the different environments from adversely impacting each other:

- a) Use different computers, partitions, and networks for development, testing, and production operations;
- b) Preclude production access to utilities and other tools such as compilers and editors that can enable unauthorized or inappropriate information access;
- c) Require staff to document any use of any system utilities, development software, or special access rights needed to make repairs then immediately revoke or remove any special rights or permissions after problem resolution;
- d) Use different IDs for development, testing, and production environments;
- e) Carefully monitor, test, and document transfers, deletions, upgrades, and promotions from development status to operational status; and,
- f) Provide for separation of duties related to the promotion from development and into production.

1.4.3 Access control to program source library

ITB utilizes a formal process to reduce the potential for corruption and to maintain the program source libraries that contain the computer programs, production source code, object code, source code listings, documentation, and operational instructions for all centralized EDD information systems. Managers responsible for maintaining any local program source libraries must document and ensure their staff maintain equivalent documentation and controls:

- a) The library must securely maintain all electronic and paper versions;
- b) The library must logically separate development, maintenance (test), and production libraries with defined configuration management practices to migrate and manage code for its life cycle and segregate data and programs to preclude opportunity to compromise operational programs;
- c) Only program librarians may make library additions, changes, or deletions for operational systems. The librarian releases only read only versions of source code. Other individuals may receive temporary authorization to perform these functions, but managers must immediately revoke authorization after revision completion;
- d) A securely maintained audit log must record all accesses and updates to development, test, and production libraries;
- e) Managers must ensure that each new or changed program operates correctly, preserves data integrity, does not adversely impact other operations, and meets ITB system requirements, coding standards, and documentation standards. Only after passing that certification, shall a program go into production with its source code, object code, test data, and test results going into the library; and,

- f) Program libraries must archive and retain old versions of source programs for at least two years. Each archive set must include a clear indication of the precise dates and times when last operational with all supporting software, job control, data definitions, procedures, test data, and test results.

1.4.4 Technical review of system software maintenance

Managers must ensure the appropriate testing of all changes to system software files prior to installation to minimize adverse operation or security impacts:

- a) Review and test all system file changes to ensure they do not compromise existing controls and or information integrity;
- b) Provide timely prior notification of all system file changes to allow appropriate reviews to take place before implementation;
- c) Ensure modification of system software setups to preclude unauthorized access (system hardening); and,
- d) Update the office continuity plan for business with any required updates resulting from system file changes.

1.4.5 Using cryptographic tools

The project risk assessment identifies information that needs encryption or application of other cryptographic controls. The ITB implements and oversees encryption and cryptographic controls to ensure:

- a) Centralized ITB oversight of all encryption and cryptographic controls to ensure consistent encryption usage, information recovery, certificate and key usage, issuance, storage, inventory, recovery, retirement, and training across EDD;
- b) Consistent procedures to address lost, missing, and or compromised encrypted information; and,
- c) Protection to ensure all contracts and service level agreements include appropriate protections for cryptographic controls if necessary; e.g., certification authority to cover issues of liability, reliability of services, and service response times (see section 4.2.2).

1.4.6 Outsourced development

When utilizing a third party to develop, acquire, modify, or install communications, networks, or systems managers must require compliance with the EDD written design requirements and utilize a contract that requires and defines:

- a) Schedule with specific measurable design and performance criteria to ensure the project remains on schedule and the contractor provides satisfactory progress;
- b) Rights for the department and a third party independent agent of the department to access and audit the quality and accuracy of work done;
- c) Licensing arrangements, code ownership, and intellectual property rights;
- d) Escrow arrangements in the event of third party failure or business collapse; and,
- e) Dispute resolution.

1.4.7 Outsourced acquisitions

Managers must require thorough testing and documentation and verify appropriate security for all new or upgrades to third party communications, networks, systems, or operational software before use:

- a) Verify third party vendor new and upgraded implementations meet EDD information security requirements and the SAM "in-use" requirements;
- b) Test and validate that the implementation meets the information security design requirements before rolling it out into production;

- c) Verify the security of the release before upgrading to a different version, e.g., the introduction of new security functionality or the number and severity of security problems affecting this version;
- d) Verify software for servers, other computers, and personal digital assistants comply with IT Circulars #00-4B - "Establishing and Maintaining the Business Driven Architecture Desktop Software Buy-List" and #01-03B - "Enterprise Desktop Software Standards for Personal Computers"; and,
- e) ITB and ISO management must require and control installation of all operational software patches that mitigate or reduce known security weaknesses.

I.4.8 Restrictions on changes to commercial software packages

EDD restricts changing commercial software packages. Modification risks compromising built-in security controls, compromising the integrity of that software, nullifying future support for the product, creating a significant future maintenance burden or risk, creating additional charges, and creating potential contracting issues. Vendors should perform all required modifications as standard program updates.

When operational requirements force changing commercial software, the ITB Deputy Director must provide advance written approval. Vendors must provide written consent and supply their source code before EDD may make source code changes to copyrighted software. Managers must ensure knowledge and skills transfer for support, provide careful acceptance testing, and retain the unmodified original software with full documentation of all changes to permit reapplying them to future software upgrades.

I.5 Acceptance of information security controls

Before acceptance of communications, networks, or systems, managers must verify incorporation of all planned security, particularly when involving confidential or sensitive information.

I.6 Application retirement

The manager responsible for a retiring communications system, network, or information system must use an appropriate formal documented process to ensure the transition does not disrupt information assets or services. This plan must ensure the appropriate disposition of all information and equipment after the transition proves successful. When retiring EDD information systems, one full copy of the latest version of the application with all relevant and enabling documentation must reside in appropriate libraries for at least two years.

APPENDIX J - SAMPLE MESSAGES

Sample security access warning message

All EDD multi-user computer systems must display a warning message when an individual attempts to access the system; e.g.:

Warning Notice!

This system is the property of the Employment Development Department (EDD) and is for official use only! Only authorized individuals with a valid business need may access it. Each individual authorized access must protect the security of the information provided. The Health and Insurance Portability and Accountability Act of 1996 (HIPAA) and California Penal Code section 502 impose severe criminal and civil penalties for any unauthorized access, use, modification, or disclosure of sensitive or confidential information. EDD prosecutes such security violations to the maximum extent permitted by law.

Sample web disclaimer message

All Internet screens, web pages, and other publicly accessible information systems must display an appropriate disclaimer message; e.g.:

Privacy Policy

The EDD provides critical mandated services that affect the health and fiscal well being of Californians. The Department recognizes that its ability to provide these services in a fair, equitable, and efficient manner depends upon a willing flow of information from its clients and business partners. Federal and State laws require carefully protecting most of this information and impose severe civil and criminal penalties for unauthorized access, use, or disclosure. Failure to appropriately protect confidential and sensitive information constitutes an information security incident. Any such incident could violate the law, seriously harm the public's trust, and jeopardize the willing flow of information that the EDD needs to deliver services. The law and EDD limit access to sensitive and confidential information to only those who have a legal right, a business need for access, and who have agreed in writing to the EDD non-disclosure policy. Further, EDD requires clients to provide a signed written request before releasing that client's information to a third party. You can learn more about [EDD privacy practices on the Web](#).

Potential Changes

Changing laws, statutes, and control agency requirements may require EDD to change or update information and web content at any time without notice. Although every effort is made to check and incorporate customer feedback, information on Web sites may contain technical inaccuracies or typographical errors. Please provide any feedback or recommended changes to the EDD web master.

Potential Risk

If you obtain a service off this web site, you automatically accept the risk of potential information compromise when using a public network. Although every reasonable precaution is taken to protect the information sent over a public network, EDD can not accept liability for its compromise, so when using the Internet and other public networks to access information, you do so at your own risk.

Business Relationships

Most EDD services are defined and governed by Federal and State laws, policies, and regulations. When you access a non-EDD Web site, even one that may contain the EDD-logo, please understand that it is independent from EDD, and that EDD has no control over the content on that Web site. EDD makes no representations whatsoever about any other Web sites which you may access through this one. In addition, a link to a non-EDD Web site does not mean that EDD endorses or accepts any responsibility for the content, or the use, of such Web site. It is up to you to take precautions to ensure that whatever you select for your use is free of such items as viruses, worms, Trojan code, and other items of a destructive nature. IN NO EVENT WILL EDD BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES FOR ANY USE OF THIS WEB SITE, OR ON ANY OTHER HYPER LINKED WEB SITE. THIS INCLUDES, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS, OR OTHER DATA ON YOUR INFORMATION HANDLING SYSTEM, OR OTHERWISE, EVEN IF WE ARE EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

APPENDIX K - REFERENCES

The following information security policy references govern this policy and were the principal documents used to formulate this policy.

- British Standards Institution, A Code of Practice for Information Security Management, Department of Trade and Industry, British Government, London, 1995 (second edition); also known as BS 7799
- California State Administrative Manual
- California Department of Finance, Technology Oversight and Security Unit (Formerly: Department of Information Technology) Information Security Policy Guidelines
- California Department of Health Services Information Security Policy
- California Public Employees Retirement System Information Security Policy
- International Organization for Standardization and the International Electrotechnical Commission Information technology – Code of practice for information security management 17799-2000-12-01
- Wood, Charles Cresson, Best Practices In Internet Commerce Security: A Standard Of Due Care Requirements List For Merchants; Publisher: PentaSafe, Houston, Texas, 1998

The following additional information security references provided policy clarification.

- American Health Information Management Association, Guidelines on Safeguards for On-line Medical Records, (includes a statement on patients' rights), 1996, write them at 919 N. Michigan Ave., Suite 1400, Chicago, IL 60611-1683 USA, or phone: 312-787-2672, 1995
- Anonymous, A Checklist of Responsible Information-Handling Practices, Privacy Rights Clearing House, University of San Diego -- Center for Public Interest Law, Fact Sheet #12, January 1995
- Anonymous, Access to and Use and Disclosure of Electronic Mail on Company Computer Systems: A Tool Kit for Formulating Your Company's Policy, Electronic Messaging Association (Arlington, Virginia), 1996
- Anonymous, Draft United Nations Manual on Computer Related Crime, September 1992, published by the Canadian Department of Justice, Ottawa, Canada
- Anonymous, Fair Information Practices Checklist, Direct Marketing Association (New York, New York), 1992
- Anonymous, Fair Information Practices Manual, Direct Marketing Association (New York, New York), 199
- Cobb, Steven, NCSA Firewall Policy Guide, National Computer Security Association, Carlisle, Pennsylvania, 1996 (www.ncsa.com)
- Corby, Michael, and Robert E. Johnston, "Intranet Security Guidelines: How To Protect The Enterprise As Your Intranet Grows," Computer Security Journal, Vol. XIV, Number 4, 199
- Computer-based Patient Record Institute Inc., Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems, (write them at 1000 E. Woodfield Road, Suite 102, Schaumburg, IL 60173 USA; or phone: 708-706-6746), February 1995
- Computer-based Patient Record Institute Inc., Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Record Systems, (write them at 1000 E. Woodfield Road, Suite 102, Schaumburg, IL 60173 USA; or phone: 708-706-6746), June 1995
- Gilbert, Gregory A., "How to Develop a Computer Security Policy," DataPro Reports on Information Security, McGraw-Hill, January 1989
- Gritzalis, Dimitris, "A Baseline Security Policy For Distributed Healthcare Information Systems," Computers & Security, Vol. 16, No. 8, pp. 709-719, 1997
- Lindup, Kenneth, "A New Model for Information Security Policies," Computers & Security, Vol. 14, pp. 691-695, 1995
- Nordic Council of Ministers (Kobenhavn, Denmark), Datapolicy: Information Security in Nordic Countries, 1993
- On Technology Corporation (Cambridge, Massachusetts, USA; www.on.com), Internet Usage and Security Template, 1997
- Overbeek, Paul, Wim Sipman, and Leon Strous, Handbook of Information Security Standards, Kluwer Academic Publishers, Dordrecht, The Netherlands (fax 078-334911), 1994
- Ozier, Will (committee chair), Generally-Accepted System Security Principles (GSSP), Exposure Draft 2.0, November 1995, published by the Information Systems Security Association, Chicago, IL (posted on www.ibm.com/security/wpconsul.htm)
- Ruthberg, Zella G., and Harold F. Tipton, Handbook of Information Security Management, Auerbach Publishers, Boston, Massachusetts, USA, 2000
- Schweitzer, James, "Classifying Information for Security," DataPro Reports On Information Security, IS15-250-101, January 1989
- Wood, Charles Cresson, "Establishing Internal Technical Systems Security Standards," Computers & Security (UK), pp. 193-200, Elsevier, Oxford, England, August 1986
- Wood, Charles Cresson, Information Security Roles & Responsibilities Made Easy; Publisher: PentaSafe, Houston, Texas, 2001
- Wood, Charles Cresson, "Principles of Secure Information Systems Design," Computers & Security (UK), vol. 9, no. 1, pp. 13-24, Elsevier, Oxford, England, February 1990
- Wright, Benjamin, The Law of Electronic Commerce: EDI, Fax, and E-Mail --Technology, Proof, and Liability, Little Brown and Company, Boston, Massachusetts, USA, 1999

GLOSSARY

Access	The ability, right, or permission to view, modify, or communicate information.
Access Control	Access controls grant or deny an individual permission to access all or part of a data resource. They help ensure that authenticated individuals and devices can perform operations only on the system resources for which they are authorized. The business rules within each application must identify what data a particular authenticated individual may view, and what operations (read, write, modify, or delete) the individual may perform.
Accountability	A protection principle that requires individual identification before permitting access to ensure violations or attempted violations can be traced to individuals and permit holding individuals responsible for their actions.
Agent/Authorized Agent	Individual or entity legally authorized to represent the data subject.
Application	A computer program or a set of programs that accomplish a business function or task.
Audit	To record independently and later examine activity under specific guidelines.
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of a sequence of activities from inception to final results. This information must include identifying source/location of access, date and time, authorized individual ID, targeted service, and activity performed.
Authentication Process (Also known as the "logon")	The second portion of the automated identification and authentication process that verifies the identity of an individual, device, or other entity, as a prerequisite to allow or deny access to system or network resources. Accessing more sensitive information requires more proof of identity. The authentication process provides the foundation for audit trails. Authentication techniques include: a) Entering a known password or personal identification number (PIN) b) Using a token, card, physical key to a lock; c) Providing a biometric; e.g., a voice print, finger print, or handwritten signature; or d) Verifying a particular location through global positioning system location.
Authorization	The granting of privileges in accordance with legal authority and the business needs of the requester to an individual, a program, or a process to allow access to an information resource.
Authorized Individual	An individual having specific limited authority from the owner of information to view, change, add to, disseminate, or delete information.
Availability	Assuring that information systems, applications, and information availability when and where needed for authorized use by authorized users.
Backup	All components including information, procedures, technology, and encryption keys needed to prevent information loss and restore services in the event of system failure or disaster.
Business Partner	External entities that enter into cooperative agreements with EDD for information exchange to facilitate the delivery of services to the public.

EDD Information Security Policy

Classification of Information	All EDD information assets must be identified and then classified as public, confidential, or sensitive in accordance with governing law and internal policy.
Confidential Information	All data associated with identifying information about a person or an entity. This includes all information that specifically identifies a person or entity; e.g., name, address, telephone number, social security number, and employer account number. The provisions of the California Public Records Act (Government Code sections 6250-6265) and other applicable state or federal laws (SAM section 4841.3) exempt confidential information from disclosure. The Administrative Manual, Information Practices Handbook (IPH), section 10-0300, contains detailed procedures for: <ul style="list-style-type: none"> a) The collection, use, storage, dissemination, and destruction of confidential information; and, b) Individual rules of conduct regarding the use and release of information.
Confidentiality	Confidentiality protects information assets against loss, and unauthorized or accidental access, use, modification, destruction, or disclosure, and carefully limits access to only those with authorization and a valid business need.
Continuity of Business	Ensuring a prioritized rapid recovery of critical business functions followed by a timely orderly recovery of all business services following a business disruption.
Continuity Plan for Business	A formal plan to protect individuals, assets, and facilities during an emergency that also provides the steps for an orderly prioritized resumption of business services following any disruption. The SAM, section 4843.1, requires EDD to maintain and periodically test its continuity plan for business. This plan identifies the most critical business functions, defines the priority in which these services are to be restored in the advent of a disruption, and identifies resources and duties with the detailed steps needed to efficiently resume all business operations.
Countermeasures	Any action, device, procedure, technique, or other measure that mitigates risk by reducing the vulnerability of, threat to, or impact on a system or information asset.
Critical Application	SAM section 4842.11 defines a critical application as those "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." Unavailability of a critical application would significantly and unacceptably affect EDD's ability to comply with its statutory mission. EDD's critical business applications and business functions include: <ul style="list-style-type: none"> a) Unemployment Insurance (UI)/Disability Insurance (DI) payment authorization and check printing; b) UI/DI new claims, recomputations, and determinations; c) Nonindustrial Disability Insurance (NDI) claims and payments processing; d) Cashiering (receipt of money); and, e) Job service placement in support of disaster recovery activities.
Critical Business Function	Same as critical application.

EDD Information Security Policy

Cryptographic Controls	Cryptographic controls protect information at risk through an encryption scheme that makes automated information unreadable without the decryption key.
Cyber Terrorism	Cyber terrorism uses malicious software and hoaxes to disrupt services.
Data	Building blocks of information. A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means. The basis of information before presentation provides meaning.
Data Classification	Process of determining whether EDD information is confidential, sensitive, or public.
Data Integrity	The accuracy and completeness of information systems and the data maintained within those systems.
Data Owner	Same as Information Owner.
Data Subject	Person or entity that which information/data pertain.
Decryption	Making information readable by unscrambling information made unreadable through encryption.
Delegated Authority	Authority granted by an authorized higher-level authority to perform specific tasks, functions, and responsibilities in relation to security of information assets.
Deputy Director	The Deputy Director owns and has primary responsibility for the information in their branch. They approve, make control decisions, and pay for information processing activities within their branch.
Desensitize	Process of removing embedded sensitive information from public records.
Digital Certificates	Digital certificates provide an automated means for an individual or firm to certify information being sent is complete and coming from them.
Digital Signatures	Digital signatures provide an automated means for offices to meet the EDD requirement to first verify the identity (authenticate) before sharing sensitive or confidential information.
Disaster	A condition in which an information asset or business function becomes unavailable as a result of a natural or man-made occurrence, and that unavailability continues for sufficient duration to cause significant disruption in the accomplishment of program objectives, as determined by management.
Disclosure	The release, transfer, dissemination, or communication of information orally, in writing, or by an automated means to any person or entity. Information releases must be in accordance with state and federal laws, the SAM and the Administrative Manual, Information Practices Handbook (IPH).
Downloading	The transfer of information from a higher level or more centralized computer system to a local computing configuration (e.g., from mainframe computer to a local area network or a desktop system, or from Internet to a PC).
Electronic Commerce	The use of electronic data interchange, electronic mail and on-line transactions to conduct business.
Emergency Response (ER)	The portion of the Operational Recovery Plan that defines the actions to ensure the health and safety of individuals following a disaster. The ER also defines necessary actions to protect critical equipment, supplies, facilities, and other resources from further damage or destruction.
Embedded Sensitive Information	Information contained within an otherwise public document that is not intended for public disclosure. Example: system logon and/or navigation procedures that are part of a directive or procedural manual.

EDD Information Security Policy

Encryption	Protective process to change plain text into an unintelligible form through use of code, cipher, translation table, or algorithm. Decryption requires the key and special process. Without encryption, confidential and sensitive information is present and at risk of being inappropriately accessed.
Essential Services	Same as Critical Business Functions.
Enterprise Level	Applicable to the entire department not just a specific program, function, or location`.
External Customer/User	All authorized individuals that are not EDD staff; e.g., general public, academics, federal, state, local, and foreign governments, UI/DI claimants, employers, Governor/Legislature, business representatives, media, publishers, software developers, community based organizations (CBO), third party service providers, third party authorized agent, and medical providers.
Firewall	A physical device that controls all network traffic to isolate segments of a computer network to protect internal networks and computers from unauthorized individuals or processes.
Guidelines	Guidelines provide information as well as suggested practices or methods for conducting business. They convey lessons learned, but are not mandatory.
Hardware	The physical computing and networking equipment that support information systems including servers, computers, and telecommunications equipment.
Identification	The first portion of the identification and authentication process where someone who requests access to information assets provides an electronic identifier or User-ID representing "whom they say they are".
Information	The presentation of data in a manner that has meaning to the recipient.
Information Assets	Information assets include all information and the individuals, facilities, services, communications, environment, technology, and media to intake, edit, process, store, sort, select, retrieve, communicate, and display information.
Information Asset Inventory	Contains at a minimum for each asset: a) Its name, description, current location, and any identification including inventory numbers; b) Its Deputy Director (information owner); c) Any system or systems that use this asset; d) Identification of which if any critical business functions are supported by this asset; e) Its security classification as public, sensitive, or confidential; f) The specific authorization requirements to be met before granting access rights; g) A list of all authorized individuals and their rights in terms of ability to view, make changes, additions, and/or deletions; h) Any special handling or dissemination requirements; and, i) The expiration date when applicable.
Information Integrity	Ensuring the accuracy, reliability, and completeness of information and information processing methods.

EDD Information Security Policy

Information Security Incident	<p>As defined in the SAM, section 4845, information security incidents are: "Incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, or access to automated files and data bases, as well as incidents involving loss, damage, or misuse of information assets"; e.g.:</p> <ul style="list-style-type: none"> a) Any unauthorized access, modification, disclosure, or dissemination of EDD sensitive or confidential information; b) Any actual or attempted violation of security policies, practices, and procedures; c) Theft, damage, destruction, or misuse of computers or related equipment; d) Unauthorized use or copying of copyrighted software; e) Unauthorized intentional access to, modification of, or use of Departmental information systems; f) Occurrence of a computer virus on a personal computer (PC), PC network, or other platform; and, g) Use of an information asset in the commission of a crime.
Information Security	The protection of information assets from loss, unauthorized access (accidental or intentionally), modification, destruction, or disclosure. Information assets will be protected based on their value, confidentiality, and/or sensitivity and the risk of loss or compromise.
Information Security Advice	The ISO oversees enterprise information security activities and provides information security advice. The ISO works closely with the ITB who coordinates in-house technical knowledge and expertise to ensure consistency, deal with security threats, provide help in security decision making, and provide information security technical advice.
Information Technology Branch (ITB)	The ITB is responsible for all EDD centralized automated information handling, including systems design and analysis, conversion of data, computer programming, information storage and retrieval, voice, video, data communications, networks, requisite system controls, simulation, and all related interactions between people and machines.
Internet	The world wide web that connects most computing equipment.
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality, or availability of an information asset.
Legal Authority	Statutory references (e.g., laws, regulations, and codes) that affect EDD.
Logical Connection	The software or application which permits entry to an information system or network.
Malicious Code	Any program or group of computer instructions that obtains unauthorized access to illegally inspect, disclose, disrupt, damage or destroy systems, networks, information, and services.
Managers & Supervisors	Deputy Directors delegate to managers and supervisors responsibility to collect, inventory, classify, process, store, distribute, maintain, protect, and ensure confidentiality, accuracy and integrity of branch information. Managers and supervisors have the most knowledge of the useful value of the information, and are the ones most affected if the information is lost, compromised, delayed, or disclosed to unauthorized parties.
Masked Data	Information about the data subject after removal of personal identifiers.
Mitigate	To do something to reduce risk to an acceptable level.
Need-to-Know	Information which can be disclosed based on business need and legal authority.
Operational Recovery Plan	See Continuity Plan for Business
Partner Entity	See Business Partner.

EDD Information Security Policy

Password	Part of the identification and authentication process where an individual provides a confidential sequence of characters to authenticate their identity, usually during a computer network logon process.
Personal Identifiers	Information stored in a record that specifically identifies an individual or entity (e.g., SSN, account number for an employer, name, and address).
Personal Information	Any information that identifies or describes an individual, including, but not limited to: name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history (Civil Code section 1798.3). It also includes statements made by or attributed to the individual.
Personnel Security	The objective of personnel security is to reduce the risks of injury, human error, theft, fraud or misuse of information assets or facilities. Personnel security should be addressed at the recruitment stage, included in job descriptions and contracts, and supervised during an individual's employment.
Physical Security	The protection of individuals, information assets, and facilities from potentially harmful situations including damage, destruction, theft, or unauthorized access.
Privacy	The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves and the right to have such information safeguarded.
Procedures	The step-by-step instructions that describe how to perform an activity. Deviation from mandatory procedures requires approval from the owner of that procedure.
Public Courier	Any of the services that EDD uses or contracts with to move information; e.g., UPS, FedEx, Western Union, etc.
Public Information	Any information prepared, owned, used, or retained by a state agency not specifically exempt from the disclosure requirements of the California Public Records Act (Government Code section 6250 et seq.) or other applicable state or federal laws. Public information includes all general information created by EDD to educate or instruct the public or staff, that is NOT classified as "confidential" or "sensitive"; e.g., directives, manuals, misc. publications, and masked data. Public information also includes information about the data subject after removal of personal identifiers. Released public information must not include encrypted data.
Record	Any file or grouping of information about an individual, which is maintained by the EDD.
Registration	Formal registration processes establish the identity, authorization, and business need for each customer to access EDD electronic systems. These processes provide customers with information security requirements, usage instructions, and obtain an appropriate signed non-disclosure agreement. They establish each valid individual "access" account with ID, initial password, and access rights. The registration processes also track customers and deactivate expired, deleted, and no longer authorized accounts.
Risk	The likelihood or probability of occurrence of an event; e.g., injury, information security incident, or loss, damage or compromise of an information asset.
Risk Analysis	The formal process of identifying and documenting assets, risks, vulnerabilities, and mitigation controls.
Risk Assessment	Identifies and weighs the consequences of potential threats or vulnerabilities that may prevent an organization from achieving its mission.

EDD Information Security Policy

<p>Risk Management</p>	<p>The formal set of risk assessment, risk analysis, and risk mitigation process, procedures, and tools to identify and document:</p> <ul style="list-style-type: none"> a) Personnel, facilities, and information assets; b) All potential personnel, facilities, and information asset vulnerabilities; c) The likelihood of each event or vulnerability occurrence; d) The potential impact, costs, and losses should an event occur; e) An alternative analysis that defines the most cost effective means to reduce risks; and, f) The formal risk mitigation plans and procedures that establish and maintain the resources, direction, and duties to remove or reduce risks to an acceptable level. <p>The SAM, section 4842, requires the Director to annually certify that EDD complies with state policy governing information technology risk management.</p>
<p>Secure Transactions</p>	<p>Secure transactions ensure protection of the confidentiality of information and financial transactions when sent over the Internet or other public communications through encrypted transmission.</p>
<p>Security Advisories</p>	<p>The ITB and ISO coordinate the release of information security alerts, required updates, virus notifications, and required activity to EDD staff and system administrators through the EDD Consolidated Services Help Desk. These alerts are known as Security Advisories.</p>
<p>Security Incident</p>	<p>See Information Security Incident</p>
<p>Sensitive Information</p>	<p>Any financial or operating information created by EDD for its own use, which is not personally identifying (confidential) that, if inappropriately released, used, or modified, could jeopardize the integrity of a system or program, or damage critical State functions. Examples include Internal audit reports, waiver and benefit determination standards, and logon procedures (SAM section 4841.3)</p>
<p>Standards (Information Technology)</p>	<p>EDD's information technology standards are infrastructure requirements. They help make inter-connectivity between work groups possible, help keep support and maintenance manageable, define standards for IT purchases, and define usage restrictions. Although information technology standards change frequently, they are mandatory as long as they are in effect. Deviation requires approval, in writing, from the ITB Deputy Director.</p>
<p>Supplemental Staff</p>	<p>Supplemental staff are defined in the Personnel Management Handbook (Section 3-1520) of the Employment Development Department to include contractors and business partners.</p>
<p>System Administrator</p>	<p>An authorized individual or organizational unit who manages and maintains automated computer systems and networks.</p>
<p>Systems Integrity</p>	<p>System integrity controls promote separation of the individuals from system processes and information, protect software, firmware, and hardware from unauthorized modifications (deliberate and accidental), and control authorized individual and maintenance personnel actions.</p>
<p>Teleworking</p>	<p>Enables staff with communications technology to work remotely outside of their organization.</p>
<p>Third Party</p>	<p>Third parties include individuals or business entities that are not employed by the EDD to assist in the conduct of EDD business functions.</p>
<p>Unauthorized Use</p>	<p>Any activity that is illegal, disrupts authorized use, compromises privacy, or destroys the integrity of information, networks, or processing capability.</p>

EDD Information Security Policy

Virus	An unauthorized insertion of a computer program or code into a computer system. See Malicious Code.
Vulnerability	The threats to which information assets may be exposed; e.g., flood, earthquake, fire, theft or loss, alteration, damage, deletion, or disclosure.