



Serving the People of California



EXTERNAL CUSTOMER ACCESS POLICY

EXTERNAL CUSTOMER ACCESS POLICY

Employment Development Department

EDD EXTERNAL ACCESS POLICY

TABLE OF CONTENTS

Page 1	Purpose
Page 1	Scope
Page 2	Guiding Principles
Page 2	Policy
Page 3	Background
Page 4	Legal Authority
Page 4	Policy Guidelines
Page 5	Security Requirements
Page 9	Responsibilities
Page 14	Definitions/Glossary

EMPLOYMENT DEVELOPMENT DEPARTMENT (EDD) EXTERNAL ACCESS POLICY

PURPOSE

The purpose of this policy is to provide a framework for maintaining data integrity and the security of EDD's information assets. This policy will enable EDD to improve customer access to EDD's services and information.

Information assets include: all information, electronic and hard copy; and information technology facilities, equipment, software, applications, telecommunications and documentation.

SCOPE

This is an enterprise level policy with guidelines for enabling external customer access to services and information, both public and confidential, in accordance with the law. It will establish minimum standards for ensuring data integrity and security and will apply to all programs, systems, and applications across the department.

The policy and guidelines will provide program managers and system/application developers with a uniform, consistent approach to designing and implementing methods to ensure data integrity and security in systems/applications.

The policy is intended to encourage, not inhibit, the development of access opportunities for our external customers. The policy enables the EDD and its customers to jointly meet their changing business needs.

The policy guidelines specify audit trail requirements for validating system security measures to prevent and detect unauthorized access.

GUIDING PRINCIPLES

<i>SERVICE:</i>	We provide efficient, quality service to our customers.
<i>SECURITY:</i>	Information is a valuable resource and must be protected.
<i>PRIVACY:</i>	Privacy is a personal and fundamental right of all persons and entities, and is protected by state and federal law.
<i>INTEGRITY:</i>	Program and data integrity are essential to the delivery of quality services.
<i>QUALITY:</i>	Our promise is to improve our products and services that meet or exceed customer expectations.

GENERAL POLICY

To meet EDD’s vision and business strategies, controlled customer access to information will be allowed in accordance with law.

All of EDD’s information must be classified as either public, confidential or sensitive. Specific policy within each classification is:

<i>Confidential</i>	Accessible only by data subject, their authorized agent, or person or entity authorized by law. Requester must be uniquely identified before access is allowed.
<i>Sensitive</i>	Will not be accessible by the public.
<i>Public</i>	Will be accessible by the public.

GENERAL POLICY

(Cont.)

Audit trails of access and access attempts will be required to prevent and detect unauthorized access, use, modification, or disclosure.

This policy requires that the policy guidelines be followed.

The policy will be reviewed periodically to ensure conformity with law and EDD vision and business strategies.

BACKGROUND

The EDD Business Plan identifies strategies to expand access to our services, build capacities to respond to new and emerging issues and opportunities, and increase communication with our customers through access to our information and services.

There is a growing demand to bring services and information to the public through multiple access points. For example, customers may have access through a variety of methods including, but not limited to telephone, Internet, kiosks, personal computers, FAX, electronic bulletin boards, and video display terminals.

Providing increased and more diverse access to EDD's information and services increases the risk that information assets could be jeopardized through unauthorized access, modification, or disclosure. To accomplish increased access while maintaining data integrity and security of information assets, EDD needs an enterprise-wide policy to ensure uniform application of security measures across programs.

**STATUTORY
AUTHORITY**

The legal authority for this policy resides in various state and federal laws:

State Law

Unemployment Insurance Code
Sections 307, 322, 1094, 1095, 2111, and 2714

Public Records Act, Government Code
Sections 6250 - 6265

Information Practices Act, Civil Code
Sections 1798 - 1798.2

Penal Code
Section 502

Federal Law

The Freedom of Information Act, 5 U.S.C.A.
Section 552, 552a

The Privacy Act, 5 U.S.C.A.
Section 552a

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

The Comprehensive Computer Data Access and
Fraud Act

**POLICY
GUIDELINES**

These policy guidelines provide specific standards and instructions for implementing the general policy. The policy guidelines are part of and carry the same weight as the general policy statement and must be followed. These policy guidelines must be updated, when warranted, to allow the application of new technologies.

The policy guidelines are divided into two parts: (1) security requirements, and (2) a matrix assigning specific responsibilities for information security and customer access.

SECURITY REQUIREMENTS

The following security requirements must be followed in designing and implementing systems that allow customer access to EDD services and information

CONFIDENTIAL INFORMATION

Confidential information includes all data associated with identifying information about a person or an entity even where encryption has been applied to the data. Examples: name, address, telephone, social security number, employer account number, etc.

Customer Service

Customer access applications must be easy to use and understand.

Access

The system must:

- Uniquely identify the requester.
- Provide a notification at initial logon that unauthorized access is prohibited by law.
- Provide an audit trail to identify who accessed the system (individual), date and time of access, targeted data, and from where (location).
- Provide confirmation to individual updating the system that the change was accepted.
- Provide a method for verification of individual accessing the system, such as Personal Identification Number (PIN), fingerprint, voice print, retinal print, or other appropriate verification method.
- Limit access to data subject or authorized agent or third party.
- Allow access only to information required by the requester's business function, and as authorized by law, and must be relevant to the business function of the requester.
- Ensure the information provided pertains only to the individual who is the subject of the request.
- Ensure that data subjects requesting information about themselves receive only information to which they are entitled.

**SECURITY REQUIREMENTS
CONFIDENTIAL INFORMATION**

(Cont.)

Access
(Cont.)

The system must:

- Advise customers who authorize release of confidential information for public viewing and use that they may have forfeited their right to privacy.
-

Data Classification

All of EDD's information must be classified as either public, confidential or sensitive.

Data Integrity

Data subjects or authorized agents will be able to update specified information in a manner determined by the data owner.

System Design

Security must be an integral part of the feasibility assessment and system design processes. The cost benefit and alternative analyses must include security design and implementation.

All applications and/or data sources developed for customer access must meet this policy's requirements.

All applications and/or data sources must be designed with a potential for customer access with appropriate security measures.

Audit Trails

A historical record of changes to client characteristics must be maintained, including from where it was changed, when it was changed, who changed it, and what was changed.

Provide capability to selectively record and monitor system activity to include access attempts and inquiry only activities, as deemed appropriate by the data owner.

Audit trails serve to prevent and detect unauthorized access, use, modification, and destruction of data.

SECURITY REQUIREMENTS

(Cont. 2)

SENSITIVE INFORMATION

Sensitive information is information created by EDD for its own use, which is not personally identifying (confidential), that is considered sensitive because public access to the information could jeopardize the integrity of a system or program. Examples: Internal audit reports, OP waiver standards, logon procedures, etc.

Customer Service

Customer access to sensitive information is not allowed.

Access

Sensitive information will not be released to the public. Customer access to sensitive information is not allowed. Example:

1. If the entire data source and/or document is sensitive, it shall not be accessed by the public.
2. If the data source and/or document contains embedded sensitive information, it must be desensitized prior to access by or release to the public.

Data Classification

All of EDD's information must be classified as either public, confidential or sensitive.

Data Integrity

Customer access to sensitive information is not allowed. Therefore, there are no data integrity issues with respect to external customer access.

System Design

All applications allowing external customer access to data sources and/or documents must provide for the ability to block access to embedded sensitive information.

Audit Trails

The system should provide the capability to selectively record and monitor access attempts, as deemed appropriate by the data owner.

Audit trails serve to prevent and detect unauthorized access, use, modification, and destruction of data.

SECURITY REQUIREMENTS

(Cont. 3)

**PUBLIC
INFORMATION**

All general information created by EDD, NOT classified as sensitive or confidential. Includes information about the data subject after removal of personal identifiers. It does not include encrypted data. Examples: Directives, manuals, misc. publications, masked data, etc.

Customer Service

Customer access applications must be easy to use and understand.

Access

Public information will be accessible to the public for reading only.

Data Classification

All of EDD's information must be classified as either public, confidential or sensitive.

Data Integrity

Information provided to the public will be accurate and current.

System Design

All applications allowing customer access to public information must provide for the ability to block access to embedded sensitive information.

Audit Trails

The system should provide the capability to selectively record and monitor data manipulation attempts, as deemed appropriate by the data owner.

Audit trails serve to prevent and detect unauthorized access, use, modification, and destruction of data.

POLICY GUIDELINES RESPONSIBILITIES

FUNCTION	RESPONSIBILITIES FOR INFORMATION SECURITY	RESPONSIBILITIES FOR EXTERNAL CUSTOMER ACCESS
<p>DATA OWNER <i>Manager of the agency or program that has primary responsibility to collect, process, store, distribute, maintain, and ensure accuracy and integrity of the information. Refer to glossary for expanded definition.</i></p>	<ul style="list-style-type: none"> • Classifying information. • Authorizing access to information by external users. • Developing security measures as required by this policy based on the classification of the information with appropriate support. • Notifying internal and external users of information of the classification of information, and requirements for maintaining security. • Approving processes which add or update data/information. • Delegating information security responsibilities to internal users. • Monitoring for compliance with policies. • Filing Security Incident Reports . 	<ul style="list-style-type: none"> • Providing program direction. • Determining cost/benefit of requested access, and determining appropriate method for information delivery. • Initiating development of new applications to meet external and internal customer access needs. • Identifying the security measures that are needed for new applications and/or data sources. • Determining cost/benefit of recommended security measures during application development or modification. • Approving new applications which will add or change data. • Providing oversight for statewide compliance with policies and procedures.

POLICY GUIDELINES RESPONSIBILITIES

FUNCTION	RESPONSIBILITIES FOR INFORMATION SECURITY	RESPONSIBILITIES FOR EXTERNAL CUSTOMER ACCESS
<p>INTERNAL USER <i>Owner of the external access point. Refer to glossary for expanded definition.</i></p>	<ul style="list-style-type: none"> • Identifying information needs of external customer or application. • Implementing security measures as required by this policy based on the classification of the information. • Applying data classification designated by owner. • Advising information users of security policies, procedures, and sanctions. • Ensuring that information needs and level of access are consistent with external customer service needs and this policy. • When delegated by data owner, taking responsibility for: <ul style="list-style-type: none"> • Authorizing access to information by external users. • Monitoring for compliance with policies • Filing Security Incident Reports. • Validating new use of data with classification criteria and with delegated authority. • Obtaining approval of data owner before implementing processes which add or update data/information. 	<ul style="list-style-type: none"> • Negotiating partnership agreements. • Implementing security policy and procedure by: <ul style="list-style-type: none"> • <i>Validating access needs of partners.</i> • <i>Verifying legal authority to access information.</i> • <i>Recommending partnership agreements.</i> • <i>Providing guidance and direction to staff in implementing policy.</i> • Providing oversight for offices' implementation of security policies and procedures. • Monitoring compliance with policies, procedures, and agreements.

POLICY GUIDELINES RESPONSIBILITIES

FUNCTION	RESPONSIBILITIES FOR INFORMATION SECURITY	RESPONSIBILITIES FOR EXTERNAL CUSTOMER ACCESS
<p>EXTERNAL CUSTOMER (Non-EDD User) <i>Refer to glossary for definition.</i></p>	<ul style="list-style-type: none"> Identifying and requesting access. Maintaining confidentiality with EDD assigned access codes. 	<ul style="list-style-type: none"> Identifying specific information needed. Providing information which will enable verification of their identity.
<ul style="list-style-type: none"> Data Subject <i>Person or entity to which information/data pertain</i> 		<ul style="list-style-type: none"> Delegating authority to an agent or third party
<ul style="list-style-type: none"> Third Parties <i>Holder of valid consent authorization from the data subject to obtain specific information regarding the data subject.</i> 	<ul style="list-style-type: none"> Demonstrating need for information. 	<ul style="list-style-type: none"> Providing legal authority for access.
<ul style="list-style-type: none"> Partner Entity <i>External entities with whom EDD enters into cooperative agreement for the exchange of information to facilitate delivery of services to the public.</i> 	<ul style="list-style-type: none"> Demonstrating need for information. Complying with terms of cooperative agreements. 	<ul style="list-style-type: none"> Providing legal authority for access.

POLICY GUIDELINES RESPONSIBILITIES

FUNCTION	RESPONSIBILITIES FOR INFORMATION SECURITY	RESPONSIBILITIES FOR EXTERNAL CUSTOMER ACCESS
<p>INFORMATION TECHNOLOGY</p> <p><i>A functional unit which has responsibility for 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.</i></p>	<ul style="list-style-type: none"> • Understanding the business needs of the owners and users of the data. • Determining how information is to be stored and retrieved. • Developing and maintaining security environment which consists of systems, networks, and applications. • Advising data owner of security and audit trail options in relation to the data. • Developing and implementing security measures as required by this policy based on the classification of the information. • Identifying new technologies which require revising these guidelines. • Notifying data owner of any actual or attempted violations of security policy. • Managing data resources and access services. 	<ul style="list-style-type: none"> • Developing new applications as requested by Program Manager and Data Owners. • Assisting Program Manager and/or Data Owners in assessing risk relative to customer access to information/applications. • Recommending solutions for application security, including costs and benefits, which meet security policy and business needs. • Updating existing applications to reflect emerging needs for customer access. • Provide support and technical assistance to ensure availability and accessibility.

POLICY GUIDELINES RESPONSIBILITIES

FUNCTION	RESPONSIBILITIES FOR INFORMATION SECURITY	RESPONSIBILITIES FOR EXTERNAL CUSTOMER ACCESS
<p>STEWARDSHIP Information Security <i>Developing and implementing policies and practices to protect information assets.</i></p>	<ul style="list-style-type: none"> • Providing guidance in determining data classification. 	<ul style="list-style-type: none"> • Providing guidance in implementation of security policies and procedures. • Participating in application development and/or modification relative to security requirements. • Coordinating changes in this policy consistent with changes in laws, rules, and regulations, and new technologies and changing business needs.
<p>Oversight <i>Formal and documented activities within the EDD designed to keep management informed of how well the organization is performing its business functions:</i></p>	<ul style="list-style-type: none"> • Providing oversight of policy implementation. • Following up on Security Incident Reports. • Investigating suspected or actual fraud or abuse. • Providing reports for administrative action and/or criminal prosecution. • Auditing for Compliance/conformity. 	<ul style="list-style-type: none"> • Maintaining oversight for compliance with security policy.

DEFINITIONS/GLOSSARY

Access Point	A logical connection permitting access to EDD's information assets or services. A kiosk is an example of a physical device that provides a vehicle for several logical connections; such as Job Service, UI claim filing, DI claim filing information, LMID data or Tax.
Agent/Authorized Agent	Individual or entity legally authorized to represent the data subject.
Audit Trails	Systems information identifying source/location of access, date and time, user-id, targeted service and activity performed.
Confidential Information	All data associated with identifying information about a person or an entity even where encryption has been applied to the data. Examples: name, address, telephone, Social Security Number, employer account number, etc.
Data	Building blocks of information. The basis of information before presentation provides meaning.
Data Classification	Process of determining whether information is confidential, sensitive, or public.
Data Integrity	The accuracy and completeness of information systems and the data maintained within those systems.
Data Subject	Person or entity to which information/data pertain.

Data Owner	The owner is the manager of the agency or program that has primary responsibility for the information. Data owners collect, process, store, distribute, maintain, and ensure accuracy and integrity of the information. They also pay for the cost of maintaining the information, 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.
Delegated Authority	Authority granted by the data owner to perform specific tasks, functions and responsibilities in relation to security of information assets.
Desensitize	Process of removing embedded sensitive information from public records.
Embedded Sensitive Information	Information contained within an otherwise public document which is not intended for public disclosure. Example: system logon and/or navigation procedures which are part of a directive or procedural manual.
Encryption	<p>A protective process which utilizes a formula or key to change information causing it to be unreadable. To read the information, the prescribed formula or key must be used.</p> <p>With encryption, personal identifying information is still present and is at risk of being read and accessed.</p>
Enterprise level	Department level, not program or function specific.

External Customer/User	All users that are not EDD staff, for example: General public, academics, federal, state, local, and foreign governments, UI/DI claimants, Governor/Legislature, employers, other states, business representatives, media, publishers, software developers, community based organizations (CBO), third party service providers, third party authorized agent, medical providers.
External Access Point	Physical location which serves as EDD's contact point with external customers.
Information	The presentation of data in a manner that has meaning to the recipient.
Information Assets	Information assets include: all information, electronic and hard copy; and information technology facilities, equipment, software, applications, telecommunications, and documentation.
Information Technology	A functional unit that has responsibility for 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.
Internal User	EDD staff and/or EDD organization that facilitates the external customer access to EDD's information (can be data owner or delegated authority).
Logical Connection	The software or application which permits entry to our information systems.
Masked Data	Information about the data subject after removal of personal identifiers.

Need-to-know

Information which can be disclosed based on business need and legal authority.

Owner of External Access Point

Internal user that:

- Receives the external request for access to department services or information.
 - Identifies a need for external access to EDD services and information.
 - Authorizes external access to services and information when delegated by the data owner.
-

Partner Entity

External entities with whom the Department enters into cooperative agreements for the exchange of information to facilitate the delivery of services to the public.

Personal Identifiers

Information stored in a record which specifically identifies an individual or entity (eg. SSN, employer account number, name, address, etc.).

Public Information

All general information created by EDD to educate or instruct the public or staff, NOT classified as “sensitive.” Includes information about the data subject after removal of personal identifiers. It does not include encrypted data. Examples: Directives, manuals, misc. publications, masked data, etc.

Sensitive information

Sensitive information is information created by EDD for its own use, which is not personally identifying (confidential), that is considered sensitive because public access to the information could jeopardize the integrity of a system or program. Examples: Internal audit reports, OP waiver standards, logon procedures, etc.

Third Party

Holder of valid consent authorization from the data subject to obtain specific information regarding the data subject.
