

 <b>California ISO</b> <small>Shaping a Renewed Future</small>	Corporate Policy Information Security	Effective Date	07/11/2011
<b>Corporate Information Security Standards</b>		Version	3.16
		Review By	07/11/2012



# California ISO

Shaping a Renewed Future

---

## Corporate Information Security Standards

	<p align="center">Corporate Policy Information Security</p>	Effective Date	07/11/2011
		Version	3.16
		Review By	07/11/2012
<b>Corporate Information Security Standards</b>			

## REVISION HISTORY

VERSION NO.	DATE	DESCRIPTION
1.0	07/10/1998	Initial Release.
1.1	08/17/1998	Minor changes to Waiver Request Form.
1.2	10/26/1998	Minor changes to Password Section.
1.3	07/15/1999	Minor changes to Password Section.
1.4	03/02/2000	Minor changes to reflect new business and org changes.
1.5	11/13/2001	Minor changes to reflect org changes and format.
DRAFT 1.5.1	03/27/2002	Review for major upgrades and linkage to other critical documents.
2.0	04/15/2002	Initial release of 2 <sup>nd</sup> version.
2.1	05/10/2002	Minor upgrades by InfoSec.
2.2	05/31/2002	Minor Upgrades to Clarify issues.
2.3	07/25/2002	Minor upgrades by InfoSec.
2.4	10/08/2002	Minor upgrades by InfoSec.
2.5	11/04/2002	Minor upgrade by InfoSec.
2.6	02/03/2003	Minor upgrade by InfoSec to reflect new Warning Notice.
2.7	05/16/2003	Minor upgrade by InfoSec regarding granting privileged access.
3.0	05/29/2003	Added sections: Telecom, Wireless, & Database. Added subsection Privileged Access.
3.1	09/02/2003	Minor Changes to Sections 11 and 14 for Clarification.
3.2	09/18/2003	Minor Change to Administrators responsibilities: 3.1.2; & 8.
3.3	10/27/2003	Minor addition to section 8.1. Short version of warning.
3.4	01/05/2004	Minor upgrade to clarify password security. ARN.
3.5	03/28/2005	Name change and updates
3.6	05/19/2005	Updated Password Matrix for UNIX to reflect standards instead of capabilities.
3.7	08/22/2005	Updated to reflect reorg
3.8	01/11/06	Updated group id
3.9	03/14/06	Exception process added
3.10	06/13/2007	Classification changed to CAISO PUBLIC. Updated organizational information for originator identification.
3.11	04/24/08	Modified section
3.12	08/06/08	Modified section 10.2.6 to include locking, archiving and deleting terminated user profiles within 30 days of termination.
3.13	06/09/09	Adding section 6.3 to document policy on remote access to ESP and added specific verbiage for password change frequency of user/service accounts.
3.14	07/21/2009	Minor grammar changes in section 6.1 and update 'Corporate User Access Security Requirements and Procedures' to 'Corporate Access Control Policy'
3.15	08/18/2010	Updated reference to the ISO using the current style guide. Validated names of documents referenced owned by other

 <b>California ISO</b> <small>Shaping a Renewed Future</small>	Corporate Policy Information Security	Effective Date	07/11/2011
<b>Corporate Information Security Standards</b>		Version	3.16
		Review By	07/11/2012

		groups and updated as required.
3.16	07/11/2011	Corrected time out and log off setting to match GPO. Updated logo and department identifiers.

 <b>California ISO</b> <small>Shaping a Renewed Future</small>	Corporate Policy Information Security	Effective Date	07/11/2011
	<b>Corporate Information Security Standards</b>		Version
Review By			07/11/2012

## TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>6</b>
1.1. PURPOSE .....	6
1.2. SCOPE.....	6
<b>2. DEFINITIONS .....</b>	<b>6</b>
2.1. STANDARD .....	6
2.2. INFORMATION .....	6
2.3. COMMUNICATIONS ENVIRONMENT AND COMPUTING INFRASTRUCTURE.....	7
2.4. INFORMATION SECURITY .....	7
2.5. REFERENCES.....	7
2.5.1. <i>Complementary Policies and Standards</i> .....	7
2.6. COMPLIANCE .....	7
2.7. EXCEPTIONS FROM CONTROLS .....	8
2.8. CHANGES.....	8
<b>3. RESPONSIBILITIES .....</b>	<b>8</b>
3.1. GENERAL RESPONSIBILITIES .....	8
3.1.1. <i>CAISO Employees, Consultants, Contractors</i> .....	8
3.1.2. <i>Application, System, database, Network Engineers, developers, and Administrations</i> .....	9
<b>4. INFORMATION SECURITY STANDARDS .....</b>	<b>9</b>
4.1. INFORMATION CLASSIFICATION .....	9
<b>5. TELECOMMUNICATIONS SECURITY.....</b>	<b>10</b>
<b>6. NETWORK SECURITY.....</b>	<b>10</b>
6.1. REMOTE ACCESS.....	10
6.2. WIRELESS TECHNOLOGY .....	10
6.3. ELECTRONIC SECURITY PERIMETER DIAL-UP ACCESS .....	10
<b>7. SYSTEM SECURITY.....</b>	<b>11</b>
7.1. WARNING NOTICE .....	11
7.1.1. <i>Caveat</i> .....	12
7.2. WINDOWS SERVERS .....	12
7.3. UNIX SERVERS.....	12
7.4. TERMINAL SERVICES SECURITY.....	12
<b>8. APPLICATION SECURITY .....</b>	<b>13</b>
<b>9. DATABASE SECURITY .....</b>	<b>13</b>
<b>10. USER SECURITY.....</b>	<b>13</b>
10.1. CONTROL IMPLEMENTATION.....	14
10.2. USER ID LIFECYCLE .....	14
10.2.1. <i>Access Criteria</i> .....	14
10.2.2. <i>User ID Inactivity</i> .....	15
10.2.3. <i>Time Out and Log Off</i> .....	15
10.2.4. <i>Functional IDs</i> .....	15
10.2.5. <i>Employee Termination</i> .....	16
10.2.6. <i>Disabling ISO User IDs</i> .....	16

 <b>California ISO</b> <small>Shaping a Renewed Future</small>	<b>Corporate Policy Information Security</b>	Effective Date	07/11/2011		
		<b>Corporate Information Security Standards</b>		Version	3.16
				Review By	07/11/2012

10.2.7.	REISSUING ISO User IDs .....	16
<b>11.</b>	<b>PRIVILEGED PASSWORD SECURITY .....</b>	<b>16</b>
11.1.	PERMISSIONS .....	16
11.2.	FORMAT AND SYNTAX STANDARDS .....	17
11.3.	PRIVILEGED PASSWORD ESCROW SERVICE .....	17
<b>12.</b>	<b>PASSWORD SECURITY .....</b>	<b>18</b>
12.1.	SECURITY REQUIREMENTS .....	18
12.2.	FORMAT AND SYNTAX STANDARDS .....	18
12.3.	DEFAULT PASSWORDS .....	19
12.4.	PASSWORD EXPIRATION .....	19
<b>13.</b>	<b>RESOURCE SECURITY .....</b>	<b>19</b>
13.1.	DATA .....	19
13.2.	MODEMS .....	20
13.3.	BACKUPS .....	20
<b>14.</b>	<b>WORKSTATION SECURITY .....</b>	<b>20</b>
14.1.	PHYSICAL SECURITY .....	20
14.2.	PRIVILEGED ACCESS .....	20
14.3.	ANTI-VIRUS SECURITY .....	21
<b>15.</b>	<b>CONTINGENCY PLANNING .....</b>	<b>21</b>
<b>16.</b>	<b>MONITORING USAGE, AUDITING, INSPECTING FILES .....</b>	<b>21</b>
16.1.	AUTHORIZED MONITORING .....	21
16.2.	UNAUTHORIZED MONITORING .....	22
<b>17.</b>	<b>INVESTIGATIONS .....</b>	<b>22</b>
17.1.	LAW ENFORCEMENT CONTACT .....	22
17.2.	INFORMATION SECURITY INCIDENT RESPONSE .....	22
<b>18.</b>	<b>COMPLIANCE .....</b>	<b>23</b>
18.1.	FIRST AND MINOR INCIDENT .....	23
18.2.	SUBSEQUENT AND MAJOR INCIDENTS .....	23
<b>19.</b>	<b>APPROVAL .....</b>	<b>23</b>
19.1.	STANDARDS APPROVAL .....	23

	Corporate Policy Information Security	Effective Date	07/11/2011
		Version	3.16
<b>Corporate Information Security Standards</b>		Review By	07/11/2012

## 1. INTRODUCTION

### 1.1. PURPOSE

The purpose of this document is to provide the California ISO (ISO) personnel with the information security standards to facilitate the implementation and management of the *Enterprise Information Security Policy* and support the *Enterprise Information Security Architecture*. This document describes the standards that must be incorporated when planning, designing, building, creating, developing, enhancing, implementing, maintaining, and using ISO networks, gateways, front-ends, information systems, applications, databases, computer-based tools, and information assets.

It is the intent of this standard to adequately protect the data and information being used, stored, processed, and transmitted within the ISO environment and communications infrastructure regardless of medium (including, but not limited to electronic, digital, radio or microwave, paper, or voice).

### 1.2. SCOPE

These information security standards encompasses all ISO personnel including employees, contractors, and consultants designing, building, maintaining and using the ISO’s information, communications environment and computing infrastructure. It also encompasses every vendor the ISO engages to conduct business as the vendor’s product and services must meet and apply these standards. Furthermore, it encompasses any entity connecting to ISO resources to conduct business.

## 2. DEFINITIONS

### 2.1. STANDARD

Standards are a set of rules that must be implemented and followed to comply with the policies. Standards provide specific details of roles and responsibilities and define standard methods and tools to be used to comply with the policies. Standards also provide additional information regarding why the policy is needed and how to implement the policies, and further explains consequences for non-compliance. The words “**must**” and “**shall**” will identify standards.

### 2.2. INFORMATION

ISO Information includes all business and corporate, as well as personnel related data and information entrusted to or created by the ISO. This includes all data and information stored, processed, transmitted, and maintained by the ISO communication environment and computing infrastructure. This information may be exempt from disclosure under provisions of the Public Record Act or other applicable State and Federal laws and tariffs.

The information can be in any medium such as electronic form (including, but limited to digital, video, softcopy, floppy diskettes, compact disks, tape, hard drives, etc.), hardcopy (paper, etc.),

	Corporate Policy Information Security	Effective Date	07/11/2011
<b>Corporate Information Security Standards</b>		Version	3.16
		Review By	07/11/2012

and transmission (including, but not limited to telephone, face-to-face conversation, Internet, wireless, electronic mail, radio or microwave, etc.).

## 2.3. COMMUNICATIONS ENVIRONMENT AND COMPUTING INFRASTRUCTURE

The ISO communications environment and computing infrastructure encompasses all networks, network devices, gateways, front-ends, information systems, applications, databases, any computer-based tools, and any communication device (wired or wireless: telephones, mobile phones, cell phones, PDA's, pagers, etc.) in which data and information is stored, retrieved, processed, and transmitted regardless of medium (including but not limited to electronic, digital, video, wireless, radio, microwave, paper, or voice).

## 2.4. INFORMATION SECURITY

Information Security is the protection of information and information systems, as well as corporate and individual privacy, by developing, implementing and managing a comprehensive security program. This program includes project planning, goal setting, requirements, risk management and is influenced by:

- State and federal laws.
- Regulatory entity regulations and tariffs.
- Business requirements and goals.
- Industry best practices.
- Industry and company policy, standards, guidelines, and procedures.

Information Security must be able to afford authentication, authorization, audit, availability, confidentiality, integrity, and non-repudiation of information and communications to confidently conduct business over any the transaction medium. The Information Security business unit is chartered to develop and manage the ISO security program.

## 2.5. REFERENCES

### 2.5.1. COMPLEMENTARY POLICIES AND STANDARDS

These information security standards support all other ISO Information Security Policies, technical standards, and the *Enterprise Information Security Architecture*.

## 2.6. COMPLIANCE

All affected ISO personnel must comply with these Standards. Any Business Unit Manager or Director who strongly believes they have a valid technological or compelling business reason for non-compliance with these Standards must prepare a written request that substantiates that belief and submit to Information Security. Information Security will perform a risk assessment and prepare recommendation to management.

Employees affected by these Standards are subject to disciplinary action for failure to comply with its terms, up to and including immediate termination of employment. Consultants and contractors affected by these Standards will be subject to termination of their contracts or requests

	Corporate Policy Information Security	Effective Date	07/11/2011
		Version	3.16
<b>Corporate Information Security Standards</b>		Review By	07/11/2012

to remove the individual offender from the ISO's premises and contract. In addition, all violations may result in the loss of some or all User privileges. Furthermore, some violations may constitute a criminal offense, as outlined in local, state, and federal laws, which the ISO will report to the appropriate authorities.

## 2.7. EXCEPTIONS FROM CONTROLS

Instances where controls cannot be met must be documented and authorized by senior management or delegate. Exceptions must be documented within thirty days of being approved by the senior manager. Documented exceptions must include an explanation as to why the exception is necessary, any compensating measures, and remediation procedures or a statement accepting risk. Authorized exceptions must be reviewed and approved annually by the senior manager to ensure the exceptions are still required and valid. Such review and approval shall be documented.

## 2.8. CHANGES

Suggestions to modify these information security standards must be submitted to Information Security to review and consider. Changes will be processed and approved in accordance with the Corporate Standards and Guidelines Creation Procedures. Each modification request must include a business case that includes:

- A description of the business or technological reason for proposing to modify this document.
- An explanation of the benefits the proposed modification can bring to the ISO.
- An outline detailing alternative considerations.

## 3. RESPONSIBILITIES

### 3.1. GENERAL RESPONSIBILITIES

Information Security is responsible for developing and maintaining the ISO Information Security Standards that provide a baseline of security requirements and specifications in support of the Enterprise Information Security Policy. Information Security is also responsible for developing and maintaining security procedures to facilitate and monitor the implementation of these security standards

#### 3.1.1. CAISO EMPLOYEES, CONSULTANTS, CONTRACTORS

ISO personnel include **all** employees (full-time, part-time, and temporary worker) currently on the ISO payroll, as well as Consultants and Contractors currently under contractual obligations. Although they are non-ISO employees, consultants and contractors are equal team players. They are under contract to complete specific projects, tasks, deliverables, or functions within a defined period.

All ISO employees, consultants, and contractors are under the same expectations and obligations to comply with the information security standards and apply the standards. In all information security documentation, ISO personnel will refer to all ISO employees, consultants, and contractors.

	Corporate Policy Information Security	Effective Date	07/11/2011
		Version	3.16
<b>Corporate Information Security Standards</b>		Review By	07/11/2012

### 3.1.2. APPLICATION, SYSTEM, DATABASE, NETWORK ENGINEERS, DEVELOPERS, AND ADMINISTRATIONS

All ISO personnel with engineering and administration responsibilities are responsible for implementing and maintaining the security standards, requirements, and procedures established by Information Security. The Developers, Engineers, and Administrators must incorporate security into their scope of work includes following the System Development Life Cycle, periodic reviews of user access lists, and the installation of security patches to all servers and workstations. They must assist in enhancing security measures and practices, as well as increasing user awareness and training. As appropriate, Information Security will assist:

- Network Engineers and Administrators to design, develop, implement and maintain an adequate level of network security in compliance with these security standards in conjunction with all other ISO Information Security Policies, technical standards, and the *Enterprise Information Security Architecture*.
- System and Application Developers, Engineers, and Administrators to design, develop, implement and maintain an adequate level of system and application security in compliance with these security standards in conjunction with all other ISO Information Security Policies, technical standards, and the *Enterprise Information Security Architecture*.
- Database Developers and Administrators to design, develop, implement and maintain an adequate level of database security in compliance with these security standards in conjunction with all other ISO Information Security Policies, technical standards, and the *Enterprise Information Security Architecture*.

## 4. INFORMATION SECURITY STANDARDS

### 4.1. INFORMATION CLASSIFICATION

The first step to ensure employee compliance with the ISO Information Security Policy is to make the employee aware of, and guide their applications of, the information classification standards. The classification of the information will determine the level of security it requires. Every employee must apply the appropriate security standards when handling classified information.

The ISO has adopted certain standards that every person in its employment must comply with. The ISO uses four classifications requiring one of the following special markings:

- **CAISO INTERNAL USE**
- **CAISO CONFIDENTIAL**
- **CAISO RESTRICTED**
- **PUBLIC**

For detailed information and instruction on how to properly classify, mark, store, distribute, transmit, destroy, secure, and handle information, please refer to the *Corporate Information Classification Standards and Protection Procedures*.

	Corporate Policy Information Security	Effective Date	07/11/2011
	<b>Corporate Information Security Standards</b>	Version	3.16
		Review By	07/11/2012

## 5. TELECOMMUNICATIONS SECURITY

Ease-of-use, connectivity, scalability, manageability, and security are critical requirements. Security measures and practices must be implemented in accordance with the Corporate Acceptable Use of Systems Policy. This will ensure the avoidance of toll fraud, service abuse and misuse.

## 6. NETWORK SECURITY

Network security focuses on establishing a logical and physical network architecture that will support an enterprise in managing security requirements. The ISO's network security architecture as described in the Enterprise Information Security Architecture, is the basis to configure secured communication links and services between databases, applications, systems, and networks based upon their classification or relative value in conducting core business processes.

Only company sanctioned equipment shall be connected to any ISO network unless approved by Information Security. To avoid technological incompatibility issues, security exposures, software incompatibility issues, and management issues, no one can connect non-company issued equipment or software. For more information, refer to the Corporate Acceptable Use of Systems Policy.

The objectives of the network security architecture are to ensure authentication, authorization, auditing, administration, availability, confidentiality, integrity, and non-repudiation. Refer to the Network Devices Security Standard.

### 6.1. REMOTE ACCESS

CAISO personnel requiring remote access must be familiar with and comply with the Corporate Access Control Policy. The ISO offers several methods to securely access resources remotely. The user must follow the process and procedures as outlined in the Corporate Access Control Policy.

Vendors conducting business with the ISO must adhere to the CAISO Vendor Remote Access Standards and Security Requirements to establish secure connections from remote sites. Any connection to the ISO network must be secured with properly configured and managed security devices such as routers, firewalls as approved by Information Security.

### 6.2. WIRELESS TECHNOLOGY

All wireless devices and technology must be approved before connecting directly to any ISO network. Information Services and other identified pertinent groups must test any wireless device or technology to ensure compatibility with existing technologies at the ISO, as well as security capabilities to comply with ISO information security policies, standards and requirements.

### 6.3. ELECTRONIC SECURITY PERIMETER DIAL-UP ACCESS

	Corporate Policy Information Security	Effective Date	07/11/2011
		Version	3.16
<b>Corporate Information Security Standards</b>		Review By	07/11/2012

The ISO does not permit dial up access to devices within an Electronic Security Perimeter. The ISO will physically audit the devices within each ESP at least annually, to verify that no dial up access is enabled.

## 7. SYSTEM SECURITY

It is important to maintain the security configuration of ISO servers. These servers store, process and transmit critical information, including CAISO Confidential or CAISO Restricted.

Privileged access must be strictly limited. System administrators will control granting higher access privileges to users in accordance with the Corporate Access Control Policy. Administrators and backups will have global access; other personnel will have least privilege access as required by their function, duties or tasks and approved by management.

### 7.1. WARNING NOTICE

While the company is not required to notify employees that they are not entitled to any type of privacy while working on ISO systems, the use of warning banners that notify all computer users, prior to gaining access to the system resources, that system usage is subject to monitoring and disclosure by appropriate site, department, or law enforcement personnel is in keeping with industry standards and security best practices.

The banner below must be displayed on the initial screen (before a user is granted any access to system resources) and require user action acknowledging their consent to monitoring and disclosure where technology permits. Warning banners are to be placed on all interactive system ports and on any non-interactive port that provides a humanly readable acknowledgment where technology permits. The warning banner provides a notice that unauthorized use is subject to administrative disciplinary action and civil and criminal penalties.

If the operating system does not have a routine facility for a system manager or user to insert an initial screen notice, other methods of notification may be used in addition to the initial and periodic user training. At a minimum, these methods must include the following:

- Posting a notice, containing the warning banner text, in a highly visible position on or near the location(s) where users may access the system, and
- Incorporation of the warning banner text in all agreements signed by the user to obtain computer system access.

This warning banner complies with the Fourth Amendment as it pertains to “Reasonable Expectation of Privacy,” the ECPA (18 U.S.C. 2702(b) & 2703(c)) as it pertains to “Accessing files stored on a server,” and Wiretap (18 U.S.C. 2511) as it pertains to “Consent to monitor real-time communications”:

-----  
\*\*\* AUTHORIZED USERS ONLY \*\*\*

This is a Private computer system. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

	Corporate Policy Information Security	Effective Date	07/11/2011
<b>Corporate Information Security Standards</b>		Version	3.16
		Review By	07/11/2012

Any or all uses of this system and all files may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site and law enforcement personnel. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

\*\*\* AUTHORIZED USERS ONLY \*\*\*

**7.1.1. CAVEAT**

In the event that it is technically not possible to use the entire warning notice as written due to character limitations, please use the following approved shortened version:

WARNING: This is a Private computer system for authorized users and uses only. Users should have no expectation of privacy. Actions on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site & law enforcement personnel. Unauthorized or improper use of this system may result in administrative disciplinary action & civil and criminal penalties. By continuing to use this system you consent to these terms & conditions, if you do not agree, LOG OFF NOW.

**7.2. WINDOWS SERVERS**

In order to ensure the proper implementation and ongoing use of security features, all critical production Windows servers at the ISO must have anti-virus and Tripwire installed. Refer to Corporate Windows Security Standards for detailed security configuration requirements.

**7.3. UNIX SERVERS**

In order to ensure the proper implementation and ongoing use of security features, all critical production UNIX servers at the ISO must have anti-virus (if technically feasible) and Tripwire installed. Refer to the appropriate UNIX Technical Standard for detailed security configuration requirements

**7.4. TERMINAL SERVICES SECURITY**

ISO users may require terminal services on their PCs to facilitate accomplishing their tasks. This standard describe the importance of installing and configuring terminal services in a secure fashion to avoid exposing ISO information to security risks or threats. This standard will help users maintain an adequate level of protection of our information in compliance with the Enterprise Information Security Policy.

	Corporate Policy Information Security	Effective Date	07/11/2011
	<b>Corporate Information Security Standards</b>	Version	3.16
		Review By	07/11/2012

When installing terminal service, it will be done in a secure fashion using an industry standard protocol used for connections between clients and servers, strong encryption, and secure configuration settings.

## 8. APPLICATION SECURITY

Application developers and administrators must follow the SDLC process to ensure proper coding and avoid programming deficiencies. The SDLC procedures include security fundamentals to ensure application exploits do not expose the ISO's information and information systems.

In addition, new applications must also comply with the *CAISO Application and CUDA-ISO Integration Standards and Guidelines* in order to take advantage of the ISO's Public Key Infrastructure (PKI) implementation. This will combine the use of encryption and digital certificates to secure access to our resources.

Privileged access must be strictly limited to a minimum. Application Administrators will control granting higher access privileges to users in accordance with the *Corporate Access Control Policy*. Administrators and backups will have global access, and all others have granular access as required by their function, duties or tasks and approved by management.

Only company sanctioned software shall be installed to any ISO workstation, laptop or server. To avoid technological incompatibility issues, security exposures, software incompatibility issues, and management issues, no one can install non-company issued software. For more information, refer to the *Corporate Acceptable Use of Systems Policy*.

## 9. DATABASE SECURITY

By applying security measures and practices in accordance to the security standards described in this document, as well as in the *Corporate Database Security Policy*. The *Corporate Oracle Database Administration Standards, Guidelines and Procedures* will ensure the preservation of our employees' privacy.

Database developers and administrators must follow the ISO's System Development Life Cycle (SDLC) to ensure proper coding and avoid programming deficiencies. The SDLC procedures include security fundamentals to ensure application exploits do not expose the ISO's data. Refer to the *Corporate Oracle Database Administration Standards, Guidelines and Procedures*.

Privileged access must be strictly limited to a minimum. Database Administrators will control granting higher access privileges to users in accordance with the *Corporate Access Control Policy*. Administrators and backups will have global access, and all others have granular access as required by their function, duties or tasks and approved by management.

## 10. USER SECURITY

Users are expected to comply with all information security policies, standards and procedures regarding the proper and ethical use of company information and resources. All employees, consultants, and contractors are responsible for the information and resources entrusted to them

	Corporate Policy Information Security	Effective Date	07/11/2011
		Version	3.16
<b>Corporate Information Security Standards</b>		Review By	07/11/2012

by the ISO and its business associates. Please refer to the Corporate Acceptable Use of Systems Policy.

A user must be granted access to only those functions or data necessary for the user to perform his or her job in accordance with the Corporate Access Control Policy. It is usually reasonable to restrict different subsets of functions and data to different users. Within technological limits, access to functions and data must be made as granular as possible. This may be done through various means such as access control lists (ACLs), tables, file access passwords or security software. Every user must have an individual user ID and password assigned to him or her to ensure accountability.

Users or their supervisors must inform the system administrators when they no longer require access to a system or application.

## 10.1. CONTROL IMPLEMENTATION

Whenever possible, implementation of user access controls must be based on a role based access control model. In this model, access decisions are based on the roles that individual users have as part of an organization. Access rights are then grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role.

In cases where a RBAC model cannot be implemented, a Discretionary Access Control model must be used. In this model, user access is based on the identity of the user in combination with the access permissions assigned by the owner.

Some database management systems provide extensive subsystems that allow access control down to the data element level. Refer to the Corporate Oracle Database Administration Standards, Guidelines and Procedures. Users may also use hardware and software configuration to control access. In other environments, the development staff may have to construct appropriate access controls.

## 10.2. USER ID LIFECYCLE

The intent of a user ID is to be a form of addressing and identification, and individual accountability. Every ISO employee and user must have an individual and unique User ID for access to resources. Sharing User IDs must not occur. User IDs must not contain intelligence, such as access codes, to identify executable transactions by the user. A user ID is important for auditing as well as tracking activities to a particular individual. Since audit reports indicate all activities (including illicit ones) associated with an ID, we need to show accountability by knowing without a doubt that who was using that user ID.

### 10.2.1. ACCESS CRITERIA

The System Administrator will create and manage the user ID. The owner of the resource to which access is being requested will grant or deny access based on the criteria described in the Corporate Access Control Policy.

	Corporate Policy Information Security	Effective Date	07/11/2011
<b>Corporate Information Security Standards</b>		Version	3.16
		Review By	07/11/2012

If different users need different levels of access, such as “read-only” or “read and update, but not delete”, the owner must document the different criteria for each level of access.

Network Administrators, System Administrators, Applications Administrators and Database Administrators and their backups are the only personnel that must have global access in order to perform their administrative duties and tasks. All other users requiring higher privileged access must be provided at a granular level and with the approval of the Director and Manager over the resource in accordance with the Corporate Access Control Policy.

Any user requiring global access privileges and is not an administrator or backup will require approval from the resource Director and Manager, as well as concurrence from the Manager of Information Security.

### 10.2.2. USER ID INACTIVITY

Administrators must disable the account of a user ID that is inactive for 90 days. This encompasses all types of accounts—system, application, database, email boxes, v-mail boxes, etc. If the user no longer needs the ID or does not contact the administrator within 30 days of the disabling, the Administrator must permanently disable the ID to ensure that folders and files are not orphaned. After 30 days of permanently disabling the ID, the Administrator must retire the ID. This will reduce the number of inactive user IDs that could expose the resource to illicit purposes.

### 10.2.3. TIME OUT AND LOG OFF

If a user ID is logged on to a client workstation, but is inactive for ten (10) minutes, then the user session must automatically invoke time-out (i.e., lock and blank the screen or security screen saver).

When the user is timed-out, the system must require re-entering the log-on password in order to resume the session. Once logged-off, the user must initiate the log-on procedure.

The user must manually invoke time-out or log-off if he or she leaves their terminal, workstation or laptop at any time.

### 10.2.4. FUNCTIONAL IDS

These IDs are set up to perform special functions by an application, individual, or a group of individuals. The user or a group must use this ID to only perform the special function; otherwise, the user must use his or her personal ID at log on. The individual’s or group’s manager is responsible for the functional ID.

When using a functional or group ID the responsible manager must ensure either automatic or manual logging controls (i.e. cameras and sign-in sheets) that shall support an audit trail of activities under this account. The responsible manager will maintain a list of all personnel by name and title that have access to this account and the list will track any staff changes. In the event of staff changes the responsible manager will ensure that the function or group ID password is changed.

	Corporate Policy Information Security	Effective Date	07/11/2011
<b>Corporate Information Security Standards</b>		Version	3.16
		Review By	07/11/2012

If a new functional ID is required, the responsible manager must use the CHASE system to request and have the Manager of Information Security approve the request.

### 10.2.5. EMPLOYEE TERMINATION

When an employee leaves employment with the ISO, the employee's supervisor or other authorized personnel must follow the Hiring and Employee Status Change Life Cycle Standard. The Human Resource Department begins the procedure by entering the termination into the employee life cycle management system.

### 10.2.6. DISABLING ISO USER IDS

Operating system IDs are disabled, rather than deleted, so the administrator can allow local management access to ensure files, folders or directories are not orphaned. Local management must reassign all files, folders or directories to a new ID within 30 days. Within 30 days of being locked after a user's termination date, Administrators must archive user profiles (both local and/or network) prior to deleting them.

If circumstances dictate expeditious deletion of an ID, the user's supervisor or manager, as well as the Manager of Physical Security Services or the Manager of Information Security must contact Human Resources (HR) to initiate the process. During an investigation by security personnel, the Manager of Physical Security and the Manager of Information Security have complete authority to dictate the status of User IDs. This includes requesting the temporary or permanent disabling of an ID during the course of the investigation.

The ID is unusable until formal confirmation is received to retire the ID. In the meantime, the supervisor must immediately complete the process via the CHASE system.

### 10.2.7. REISSUING ISO USER IDS

If the ID of a new employee, consultant or contractor is a duplicate of a disabled ID, then follow the uniqueness format (per the ISO Naming Standard). If an employee returns to the ISO (out of retirement, contractor rehired), then their old ID must be reissued.

## 11. PRIVILEGED PASSWORD SECURITY

Administration and production support personnel need special privileges on the systems for which they are responsible. Administrators need to be able to add, activate, deactivate and delete user IDs and passwords. They need to make table changes and audit their systems. Production support personnel need to correct corrupted data elements, allocate and de-allocate files, or start and stop processes. Network administrators need to access controllers to manage the network.

### 11.1. PERMISSIONS

Permission to perform such specialized acts may be granted through normal access control mechanisms of the application. Permission must be obtained only when needed, and access to a

	Corporate Policy Information Security	Effective Date	07/11/2011
		Version	3.16
<b>Corporate Information Security Standards</b>		Review By	07/11/2012

super user or privileged state is provided by a special password. When the super user or privileged state is no longer required, the user must exit or log-off the privileged state.

Administrators and backups must have global access. All others must have limited privileged access rights according to the need to perform assigned functions, duties or tasks in accordance to the Corporate Access Control Policy.

## 11.2. FORMAT AND SYNTAX STANDARDS

Super user or privileged state passwords must meet the password standards described in the Password Security section of these standards. In addition:

- Change it every **90** days on network devices and on all other systems, regardless of any changes within the change interval.
- Change it whenever a super user or privileged user leaves the job or no longer needs the access.
- Administrators shall provide Information Security with a copy of the password. The password must be in a double sealed envelope and placed in a secured safe accessible only by authorized Information Security personnel. Machine and account will identify the envelope. The intent is to provide a password escrow service.
- Administrators must escrow the password every time it changes.
- The Administrator must provide Information Security with a list of users with this password. The list must be updated with any change (delete names, add names, change access) as soon as possible.
- Keep super users or privileged users to a minimum, (i.e., those with a need-to-know). Special system commands must be restricted only to administrators, e.g., in the UNIX system ‘SU’, to grant privileged status.

## 11.3. PRIVILEGED PASSWORD ESCROW SERVICE

Administrators shall provide Information Security with a current list of users granted super user or privileged user status. The Administrators must keep this information current; therefore, updates must be made whenever a change occurs.

The Administrators shall also provide a current list of the super user password per machine and per account in a double sealed envelope. Information Security shall store the lists and envelopes in the Folsom Information Security data safe.

This process will provide management with a fail-safe process in the event that all authorized administrators are unreachable to grant privileged status or to access that state. The Information Security personnel shall not open the double sealed envelope at any time. The envelope will be hand delivered by authorized Information Security personnel to the user seeking the privileged password. The user must have his or her Director’s approval to request the privileged password.

On the following business day, Information Security will inform the appropriate Administrator that an emergency existed and that Information Security had to provide the privileged password. The Administrator will follow up and either adds the employee to the list of users requiring the

	Corporate Policy Information Security	Effective Date	07/11/2011
<b>Corporate Information Security Standards</b>		Version	3.16
		Review By	07/11/2012

privileged password or change the password. The administrator must then escrow the new password. For more information on escrowing privileged passwords, refer to the *Privileged Password Escrow Services Policy and Procedures*.

## 12. PASSWORD SECURITY

A password, in conjunction with an ID, is the primary means of identifying and authenticating an individual. Every user must be assigned an individual and unique user ID and password. Each user ID must be associated with a unique password to authenticate and grant authorization, as well as to record activity performed by that access event. The Administrator shall also provide the users with their initial passwords that must be changed by the users first time it is used. Each owner of an ID shall be responsible for keeping his or her password secret.

### 12.1. SECURITY REQUIREMENTS

Logon procedures and password change procedures must automatically suppress or fully blot out passwords. Unless specifically required by the application, passwords must not be embedded or hard-coded in clear text or otherwise including, but not limited to, keyboard keys (e. g., the record/playback keys on UNIX keyboards), function keys, automated systems and logon scripts from workstations or laptops.

Passwords must be transmitted or stored in encrypted form. To prevent password cracking programs from finding passwords, files containing encrypted passwords must not be readable by non-administrators. Encrypt all text files and email messages containing a password or password lists.

System Administrators shall unlock or reset user passwords in such a way that the user's identity is established and the password provided to them in a secure manner. The ISO Support Center, in conjunction with Information Security, must develop and manage the *ISO User Identification for Password Resets* procedures and adhere to all user ID and password security standards and procedures.

### 12.2. FORMAT AND SYNTAX STANDARDS

Implementation of the following password standards and requirements are subject to the restrictions of the operating systems or security software. The intent of these standards and requirements are to maximize ease-of-use without sacrificing security for all ISO personnel accessing the ISO's communications environment and computing infrastructure. Password minimum-security requirements are defined below and include:

- Passwords must not be less than 8 characters.
- Passwords must not equal a dictionary word.
- Passwords must contain at least one uppercase character.
- Passwords must contain at least one numeric character.
- Passwords must contain at least one special character.

	Corporate Policy Information Security	Effective Date	07/11/2011
		<b>Corporate Information Security Standards</b>	Version
		Review By	07/11/2012

All software and applications not directly capable of enforcing these standards are required to implement the most strict password complexity requirements the specific technology is capable of enforcing.

**UNIX Password Standard** – Refer to the appropriate *UNIX Security Standard*

**Windows Password Standard** – Refer to the *Windows Security Standard*

**Oracle Password Standard** – Refer to *Corporate Oracle Database Administration Standards, Guidelines, and Procedures*

**LDAP Password Standard** – Applications that consume LDAP users for username/password authentication receive their credentials via Active Directory replication. By default, Active Directory enforces the strictest password complexity possible.

**Voicemail** – Voicemail passwords must be a minimum of five characters in length. After 5 consecutive unsuccessful login attempts to voicemail, the account will be locked and the user must contact user support to have the account reset.

### 12.3. DEFAULT PASSWORDS

Many software products require password to use their special facilities, and such products arrive with default password values. All vendor-supplied passwords must be changed when products are installed.

### 12.4. PASSWORD EXPIRATION

Unless specifically defined in alternate policy or standard, all operating system accounts for users and services will be change every 90 days. The standard implementation of this requirement will be through the integration of the system or device with an enterprise authentication system (such as Active Directory or Oracle Internet Directory).

Due to technical limitations with integrating with the enterprise authentication systems on UNIX systems, user accounts and service accounts will be changed annually until these systems can be integrated.

## 13. RESOURCE SECURITY

Excessive personal use, abusive use, misuse, obstructive use and inappropriate use of company resources may be subject to disciplinary action up to and including dismissal. For additional information, please refer to the *Corporate Acceptable Use of Systems Policy*.

### 13.1. DATA

All data stored, processed and transmitted in the ISO computing infrastructure and communications environment (including, but not limited to computers, network resources, electronic mail, voice mail, passwords, and fax machines) are company property and are subject to inspection without notice. Refer to the *Enterprise Information Security Policy*.

	Corporate Policy Information Security	Effective Date	07/11/2011
<b>Corporate Information Security Standards</b>		Version	3.16
		Review By	07/11/2012

Date stored, processed and transmitted must comply with the Corporate Information Classification Standards and Protection Procedures.

## 13.2. MODEMS

Workstations, laptops, or servers connected to any ISO network must not use unsecured modems. All modems must only use dial-out lines and turn off modems when not needed. Users must complete a CHASE Request indicating the business need for the modem and location of the modem connection. The Manager of Information Security Services must review and approve the completed CHASE Request.

If the user needs dial-in and out service, they must submit a strong business case including how they will secure the access. The Manager of Information Security Services must approve the request.

## 13.3. BACKUPS

The ISO Administrators must back-up their systems and store them at a reputable off-site storage company. The storage-company must ensure the confidentiality and integrity of the backup tapes at their off-site facilities. The Administrators may recycle the backup tapes by irretrievably erasing or overwriting them. Alternatively, they may destroy the disks or tapes when no longer required. Refer to the CAISO Records Management Policy and the CAISO Records Retention Schedule.

## 14. WORKSTATION SECURITY

### 14.1. PHYSICAL SECURITY

Protect desktop workstations and laptops from unauthorized use or removal. In addition, every employee using a workstation or laptop and its associated materials including software, diskettes, and printer output, shall be responsible for applying the security measures outlined in the Corporate Information Classification Standards and Protection Procedures.

Users shall comply with all applicable standards regarding use of equipment.

### 14.2. PRIVILEGED ACCESS

In order to maintain a consistent software version level set throughout the enterprise and to ensure only authorized software is installed in our computing environment, only the User Support Services support personnel shall have administrative rights to all machines issued by the ISO. Support personnel include all Windows Administrators and their backups, Desk Side Support Personnel and others identified by the Information Security.

It is the ISO standard that all non-support ISO personnel assigned ISO issued machines must not have privileged access (admin rights to the machine networked or local).

	Corporate Policy Information Security	Effective Date	07/11/2011
	<b>Corporate Information Security Standards</b>		Version
Review By			07/11/2012

A user requiring privileged access (admin rights) must provide justification and obtain approval from their Director and Manager. Users must request this privileged access in accordance with the Corporate Access Control Policy.

### 14.3. ANTI-VIRUS SECURITY

All workstations shall use anti-virus software to prevent computer virus infection. The software should scan all disks when inserted and before downloading, executing programs or opening files. Computer viruses are programs that replicate themselves onto other programs or files. Most are nuisances, but some are very malicious. Virus programs can use all available space, display messages, modify data, delete files, reformat disks, or change file formats. Refer to the Malicious Software Prevention Program and Procedures.

## 15. CONTINGENCY PLANNING

New projects designing new applications, systems, or networks must include contingency plans as an integral part of their project plan and design. The project or product manager must consult with Lead Strategic Contingency Planner to ensure compliance. The project's sponsoring Officer must approve the contingency plans preferably during the development phase. This will avoid costly and potentially disruptive retrofitting efforts.

The Lead Strategic Contingency Planner will work with the projects to document the coordination and planning of their contingency planning efforts. All corporate plans must incorporate the Corporate Information Security Standards to comply with the Enterprise Information Security Policy.

For additional information on the ISO BCP efforts, refer to the Emergency Management Program. All ISO personnel must be familiar with their Contingency Plans.

## 16. MONITORING USAGE, AUDITING, INSPECTING FILES

### 16.1. AUTHORIZED MONITORING

Management has the right, per the Enterprise Information Security Policy, to monitor use and will perform periodic auditing of all equipment and software provided to all Authorized Users without prior consent of, or notification to the user including, but not limited to:

- Personal observation.
- Complaint from another User.
- Comment as result of observation by an administrator during the normal performance of his/her job function or assignment.
- Comment from the Information Security Department employees as the result of an investigation into a security incident.
- Comment from the Information Security Department employees resulting from periodically performed spot checks of system usage.
- Comment from Human Resources employees or the ISO Legal Department as a result of an investigation into harassment, discrimination, performance or other related issues.

	Corporate Policy Information Security	Effective Date	07/11/2011
		Version	3.16
<b>Corporate Information Security Standards</b>		Review By	07/11/2012

- Results from software, hardware, and network monitoring tools.

## 16.2. UNAUTHORIZED MONITORING

Authorized Users may not use computing resources or network analytical equipment or software to monitor electronic communications. This would be an unauthorized use of equipment or services and will be considered a security incident and investigated by Information Security in cooperation with Human Resources and Legal.

## 17. INVESTIGATIONS

Information Security is responsible to manage and lead investigations of information security incidents, violations, and breaches. Information Security will lead and manage the investigation in accordance with the *Information Security Incident Response Team Procedure (ISIRT)*.

### 17.1. LAW ENFORCEMENT CONTACT

If any ISO personnel is contacted by a representative from an external law enforcement organization (District Attorney's Office, FBI, Police Department, Sheriff's Office, ISO security officials, etc) that is conducting an investigation on alleged violations involving ISO computing and networking resources, they must redirect, refer, or transfer the inquiry to Information Security immediately.

### 17.2. INFORMATION SECURITY INCIDENT RESPONSE

All Authorized Users share a measure of responsibility in intrusion detection, prevention, and response. Information Security has been delegated the authority to enforce information security policies and is charged with:

1. Implementing system security architecture mandates, system protection features, and procedural information security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.
2. Initiating appropriate and swift action, using any reasonable means, in cases of suspected or alleged information security incidents to ensure necessary protection of company resources, which may include disconnection of resources, appropriate measures to secure evidence to support the investigation of incidents, or any reasonable action deemed appropriate to the situation.

All ISO personnel have the responsibility to report any discovered unauthorized access attempts or other improper usage of ISO computers, networks, or other information processing equipment. If you observe, or have reported to you, a security or abuse problem with any ISO computer or network facilities, including violation of this procedure, you should take immediate steps as necessary to ensure the safety and protection of ISO resources. For example, if warranted, a system administrator should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network.

Ensure that the following people are notified:

	Corporate Policy Information Security	Effective Date	07/11/2011
		Version	3.16
<b>Corporate Information Security Standards</b>		Review By	07/11/2012

1. Information Security;
2. Your manager or contract manager; and
3. Your support representative.

Information Security will coordinate the technical and administrative response to such incidents in accordance with the *Information Security Incident Response Team Procedure (ISIRT)*.

## 18. COMPLIANCE

All ISO personnel must comply with this policy and adhere to and apply these standards. Employees affected by this policy and standards are subject to disciplinary action for failure to comply with its terms, up to and including immediate termination of employment. Consultants and contractors affected by this policy and these standards will be subject to termination of their contracts or requests to remove the individual offender from the ISO's premises and contract. In addition, all violations may result in the loss of some or all User privileges. Furthermore, some violations may constitute a criminal offense, as outlined in local, state, and federal laws, which the ISO will report to the appropriate authorities.

### 18.1. FIRST AND MINOR INCIDENT

If an Authorized User has violated this policy or these standards, and (1) the violation is deemed minor in the sole discretion of Human Resources (for employees) or Finance (for contractors and consultants) and/or the Information Security Department, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the Business Unit level. The alleged offender will be furnished a copy of the *Enterprise Information Security Policy* and the *Employees Code of Conduct and Ethical Principles* and reminded that he or she signed them acknowledging compliance with the policy upon employment.

### 18.2. SUBSEQUENT AND MAJOR INCIDENTS

Reports of subsequent or major violations will be forwarded to Human Resources (for employees) or Finance (for contractors and consultants) and the business unit Officer(s) by the Information Security Department for investigation and appropriate action. Human Resources, Legal and/or Finance may give guidance regarding appropriate action.

## 19. APPROVAL

### 19.1. STANDARDS APPROVAL

This Standard was created under a stakeholder process.

#### Responsible Manager

**Robert Melis, Manager of Information Security**

Print Manager's Name and Title

**x 2372**

Telephone