 <b>California ISO</b> <i>Shaping a Renewed Future</i>	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
<b>Information Classification Standards          And Protection Procedures</b>		Version	2.9
		Review By	06/21/12




# California ISO

*Shaping a Renewed Future*


---

## **Information Classification Standards And Protection Procedures**

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	


## REVISION HISTORY

VERSION	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	12/19/2001	Major Re-Formatting, Separated From Main Document into Individual Document.
DRAFT 1.5.2	02/04/2002	Minor Revisions by HR, Legal and Project Office.
DRAFT 1.5.3	04/29/2002	Final Draft for Final Review
DRAFT 1.5.4	05/08/2002	Minor upgrades, final review.
2.0	05/15/2002	Initial Release of 2 <sup>nd</sup> Version
2.1	09/12/2003	Minor format upgrades, no other changes.
2.2	03/04/2005	Added the CEII and PCII Classification and other minor revisions by Information Security
2.3	08/01/2005	Added the new organizational abbreviations
2.4	04/05/2006	Changed IS to IT
2.5	08/09/2007	Public modified
2.6	01/09/2009	Modified compliance section to state annual monitoring. Changed document owner to Robert Melis.
2.7	02/06/2009	Included section for protection of CIP information related to Critical Cyber Assets with information examples.
2.8	05/04/2009	Revised Appendix B Department Abbreviation Codes to be based on an algorithm using the current organizational hierarchy to reduce updates to the document.
-	05/05/2010	Reviewed, no changes required.
2.9	06/01/2010	Updated Appendix A, CAISO CONFIDENTIAL handling instructions to indicate that data should be “physically locked up” instead of “out of site”.
-	6/21/2011	Updated logo and org information in footer. Some grammatical changes. No other changes required. Annual review by Tim Lockwood.

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

## Table of Contents

1. PURPOSE .....	4
2. SCOPE.....	4
3. STANDARD .....	4
3.1 Roles and Responsibilities.....	5
3.2 Information Requiring Enhanced Protection.....	7
3.3 Classification Levels and Protection Measures .....	8
3.4 Classification Labeling and Control Statements .....	9
3.4.1 Public.....	9
3.4.2 CAISO Internal Use .....	9
3.4.3 CAISO Confidential .....	9
3.4.4 CAISO Restricted.....	10
3.4.5 PCII/CEII.....	10
3.5 Originator/Author Identification.....	10
3.6 Disclaimer Usage.....	11
3.6.1 Facsimile Disclaimer Notice .....	11
3.6.2 Electronic Mail Disclaimer Notice .....	11
3.6.3 Posting Disclaimer Notice .....	12
3.7 Distribution of ISO Operating Procedures .....	12
3.7.1 Determination of Sensitivity.....	12
3.7.2 Assignment of Sensitivity Codes K, S, and P.....	13
3.7.3 Description of Codes K, S, and P .....	13
3.8 Attorney-Client Communications .....	14
3.8.1 Approved Notice .....	15
3.8.2 Notice Format.....	15
3.8.3 Proper Use .....	15
3.9 Intellectual Property .....	15
3.9.1 Copyright Marking .....	15
3.9.2 Trademarks .....	16
3.9.3 Patents .....	16
3.10 Declassifying Information .....	16
4. INCIDENT REPORTING.....	16
4.1 General Security Breaches .....	16
4.2 Computer Security Breaches .....	17
5. CHANGES AND MODIFICATIONS .....	18
6. COMPLIANCE .....	18
Appendix A - Classification Levels and Protection Measures .....	19
Appendix B - Department Abbreviation Codes .....	24

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

## 1. PURPOSE

The purpose of this document is to support the *Enterprise Information Security Policy* by defining the information classification and describing protection procedures. The California ISO is committed to protecting the security and privacy of information, regardless of media type, in accordance with applicable laws and regulations. Information is a critical and valuable asset for the California ISO. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. The objective of information security is to reduce the risk to the California ISO and Market Participants by protecting information, information systems and communications that deliver the information, from failures of integrity, confidentiality, and availability, whether information is in storage, processing, or transmission. Information security is seen as an enabler to achieve California ISO business strategy and objectives and to avoid or reduce relevant risks.

This standard:

- Identifies information that requires enhanced protection and security under federal and state law, the California ISO Tariff, the California ISO Information Availability Policy, and applicable regulations
- Describes methods to provide physical and technical security of such information
- Explains roles and responsibilities
- Describes the obligations for reporting security breaches that violate this policy


Questions regarding implementation of this standard should be directed to the California ISO Information Security Department.

## 2. SCOPE

This policy encompasses all California ISO employees, consultants, contractors, and vendors, hereinafter described as “California ISO personnel”, “personnel” or “Authorized Users,” conducting business with the California ISO. In addition, all third parties, including vendors, who have access to or control of California ISO information described in this standard, must agree in writing to maintain such information confidentially and in accordance with federal and state laws, the California ISO Tariff, the California ISO Information Availability Policy, and applicable regulations, as described in further detail in this standard.

## 3. STANDARD

All California ISO information shall be classified, labeled, protected, and handled as described in this standard. This standard identifies information classification and information that requires enhanced protections under federal and state law, the *California ISO Tariff*, the *California ISO*

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

*Information Availability Policy*, and applicable regulations. Stewards, Managers, and Authorized Users of such information all have obligations to identify such information and take precautions as required in this standard to ensure that such information is protected. Section 3.2 describes the roles and responsibilities of Stewards, Managers, and Authorized Users in further detail.

Documents where classification labels have not been applied will always be considered “Confidential” and must be handled as such.

All California ISO personnel who have access to California ISO information is expected to exercise discretion, common sense and reasonable judgment in connection with their use of information created, stored, transmitted or disposed in the course of their job duties, regardless of the medium in which that information is maintained.

### **3.1 Roles and Responsibilities**

All California ISO personnel share in the responsibility for protecting information. This section of the policy defines and describes those groups that have particular responsibilities in this regard:

#### **3.1.1 Originator**

The originator of information is responsible for classifying and ensuring that the appropriate security standards and procedures are properly applied.

#### **3.1.2 Stewards**


Stewards are California ISO personnel who have responsibility to maintain and control particular California ISO generated and/or maintained information. Stewards oversee and manage the official repository of such information and, therefore, are responsible for the integrity, confidentiality, and availability of that data (e.g., Market data, Human Resources for employee records, etc.). Stewards have a responsibility to use reasonable efforts to ensure that other individuals and third parties who receive such information understand their respective rights and responsibilities in using and transmitting the information to others. Joint stewards are mutually responsible for such information.

#### **3.1.3 Managers**

Managers are responsible for ensuring that their unit has completed education regarding information security, overseeing compliance with California ISO policies and procedures in this regard, and immediately reporting breaches of this policy to the Information Security Department.

“Managers” and “Stewards” are expected to oversee User compliance with this and other information security policies.

#### **3.1.4 Users**

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

All California ISO personnel are “Users” even if they do not have responsibility for managing the resources. Users are responsible for protecting information resources of which they have access. Their responsibilities cover both computerized and non-computerized information and information technology devices that are in their care or possession. They shall follow the information security policies and procedures as well as any departmental or other specific applicable information security practices.

Users are responsible for completing education regarding information security, adhering to the California ISO’s policies and procedures regarding information security and reporting breaches of the policies to the Information Security Department.

“Users” of personal or sensitive information or information protected under federal and state law are expected to comply with the procedures to implement this policy, as appropriate, to protect privacy and security of such information.

### 3.1.5 Vendors and Other Third Parties

Vendors and other third parties that access California ISO information covered under this policy are required to comply with the applicable privacy and security regulation and requirements set forth in this policy. California ISO personnel shall take reasonable and appropriate steps to ensure vendor compliance through contractual requirements.


Vendor’s non-compliance with this policy shall be reported to the appropriate supervisor or individual responsible for overseeing the vendor as well as the Manager of Information Security.

### 3.1.6 Manager of Information Security

The Manager of Information Security has primary responsibility for oversight of information security, security policy and procedure development, revision and oversight, implementation of the California ISO’s information security plan and educating the community about security responsibilities.

All incidents of actual or suspected security breaches must be reported immediately to the Information Security Department. The Manager of Information Security will investigate the incident and coordinate with necessary members of the California ISO and will comply with federal and state law requirements regarding incident reporting and notice as set forth in this policy.


The Information Security Department shall issue policies, procedures, and additional guidance to assist the California ISO personnel in implementing this and other information security-related policies. This policy is the umbrella policy for future policies and procedures related to information security.

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

### 3.2 Information Requiring Enhanced Protection

The following describes information that requires enhanced protection. California ISO personnel who create, use, transmit or dispose of information in any of the following categories are expected to appropriately maintain the confidentiality of such information in accordance with this standard as well as federal and state law, the California ISO Tariff, the California ISO Information Availability Policy, and applicable regulations.

- *“Protected Health Information,”* created or received by a health care provider that: (1) identifies an individual; and (2) relates to that individual’s past, present or future physical or mental health condition or to payment for health care. Protected Health Information is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- *“Personnel Records,”* protected under state law, which include letters of offer, employment records, salaries, fringe benefits, and other personnel information.
- *“Personal Information,”* protected under state law. The California Database Protection Act (CDPA, formerly known as SB 1386) and AB 1950 applies to California residents and protects an individual’s first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  - Social Security number.
  - Driver’s license number of California Identification Card.
  - Account number, credit or debit card number, in combination with any required password, security or access code that permits access to the individual’s financial account.
- *“Intellectual Property,”* that are protected by copyright, trademark, trade secret, patent or other intellectual property right. The California ISO is the owner, pursuant to federal and California law, of all intellectual property created by California ISO personnel which is:
  - Created or developed during the course of an individual’s responsibilities to California ISO, including works made for hire; or
  - Created or developed pursuant to a sponsored agreement or pursuant to a written agreement to transfer ownership to California ISO; or
  - Created or developed with the significant use of California ISO facilities, funds, resources or supplies.
- Records that contain information required to be kept confidential or otherwise not subject to disclosure by the Corporation’s Articles of Incorporation, bylaws, or by any tariff or agreement accepted by FERC for filing and currently in effect. Such records include, without limitation, individual bids for supplemental energy and ancillary services, individual adjustment bids for congestion management that are not designated by a scheduling

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	

coordinator as available, transactions between scheduling coordinators, individual generator outage programs, and market monitoring activities.


- Records pertaining to matters properly discussed in a closed/executive session in accordance with the Corporation’s Open Meeting Policy then in effect.
- Records that refer to commercially sensitive matters, disclosure of which may affect the competitive positions of the Corporation’s market participants, or otherwise compromise the efficiency of the market as a whole or of the efficient and nondiscriminatory access to the transmission grid.
- “*Critical Infrastructure Protection (CIP) Information*” associated with Critical Cyber Assets, regardless of media type, shall be treated as CAISO Confidential. This information shall include:
  - Operational procedures for Critical Cyber Assets
  - The Critical Asset List and Critical Cyber Asset List as required in CIP-002
  - Network topology or similar diagrams for Critical Cyber Assets
  - Floor plans of computing centers that contain Critical Cyber Assets
  - Equipment layouts of Critical Cyber Assets
  - Disaster Recovery plans for Critical Cyber Assets
  - Incident Response plans for Critical Cyber Assets
  - Security configuration information for Critical Cyber Assets

### 3.3 Classification Levels and Protection Measures

The California ISO has five information classifications – CAISO Public, CAISO Internal Use, CAISO Confidential, CAISO Restricted, and PCII/CEII. The official CAISO classification markings are as follows:

- CAISO PUBLIC
- CAISO INTERNAL USE
- CAISO CONFIDENTIAL
- CAISO RESTRICTED
- Protected Critical Infrastructure Information (PCII) / Critical Energy Infrastructure Information (CEII)

The table located in Appendix A will assist in classifying and protecting information appropriately. Prior to classifying information as PCII or CEII it first must be approved by Legal and Information Security. In the event your unable to determine the proper classification or unsure how to protect information, contact Legal or the Information Security Department.

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

### 3.4 Classification Labeling and Control Statements

It is important to properly label information in order for the user to know how to protect it. Classification labels must follow a standard format:

- Marking must appear on the bottom center of the page or computer screen.
- Marking must appear on diskette and other removable media labels.
- Control Statements must appear on the bottom center of the page or screen directly below the official marking.

The purpose of the Control Statement is to inform the user of additional requirements regarding the restrictions and handling of that information. They should be used when the information steward or originator deems it necessary to add additional information to restrict the handling of that information. The Control Statement must appear directly beneath the classification marking. The following lists each control statement and examples of use.

The work and investment by ISO personnel to create or develop information may also be considered intellectual property requiring copyright protection. Refer to Section 3.9, Intellectual Properties for more information about using the copyright mark.

#### 3.4.1 Public

- Copyright.

<b>CAISO PUBLIC</b> COPYRIGHT © 2003-4 by California ISO. All Rights Reserved.
---


#### 3.4.2 CAISO Internal Use

- Not to be released or disclosed outside the ISO. Do not release or disclose outside the ISO.

<b>CAISO INTERNAL USE</b> For use by all authorized CAISO personnel. Do not release or disclose outside the CAISO
---

#### 3.4.3 CAISO Confidential

- For use by authorized ISO personnel with a need-to-know. Do not release or disclose outside the ISO.

	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
	<b>Information Classification Standards And Protection Procedures</b>	Version	2.9
		Review By	06/21/12

- Not to be released or disclosed outside the CAISO and (name of other company) without a signed confidentiality and non-disclosure agreement<sup>1</sup>.

**CAISO CONFIDENTIAL**  
For use by authorized CAISO personnel only with a need-to-know.  
Do not release or disclose outside the CAISO.

### 3.4.4 CAISO Restricted

- This information is for use solely by authorized ISO personnel and (name of other company) employees with a need-to-know and a signed non-disclosure agreement. Do not release, disclose or reproduce this information. Refer inquiries or copy requests to the steward.
- For use by authorized ISO personnel with a need-to-know. Do not release, disclose, or reproduce this information.
- For your use ONLY  
Assigned To: (NAME) [on first page only]  
Do not release, disclose or reproduce this information.

**CAISO RESTRICTED**  
This information is for use solely by authorized CAISO and Bailey, BOW, and n-Cipher employees with a need-to-know and a signed confidentiality non-disclosure agreement. Do not release, disclose or reproduce this information.  
Refer inquiries or copy requests to John Smith.  
[On each page] [On first page only]

### 3.4.5 PCII/CEII


The Department of Homeland Security and the Federal Energy Regulatory Commission applies the necessary markings upon the submittal and acceptance of the PCII Package.

**PCII or CEII**

## 3.5 Originator/Author Identification

The originator/author of documents must identify themselves so employees know whom to contact to ask questions, to request copies, or to return the document. The originator/author must place his or her initials at the bottom left hand corner with his or her Department's abbreviation. Use this coding scheme on all documents that do not clearly identify the originator/author. For example, an interoffice memorandum already indicates "From", but a document attached to the memo must contain the identification in case the cover memo and document become detached.

<sup>1</sup> Employees may obtain a non-disclosure agreement (NDA) template from the Legal Department. Legal will assist in completing the NDA.

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

This scheme does not replace the classification markings or control statements, but enhances the ability to identify the document originator/author (see footer on this document as an example).

The approved department abbreviation codes are located in Appendix B.

### 3.6 **Disclaimer Usage**

Using disclaimer notices enhances the ISO's due diligence in attempting to do the right thing to protect information. Adding disclaimer notices to message transmitted electronically may enhance the security and privacy of that information during legal proceedings. Communication transmissions include, but not limited to facsimile machines and electronic mail over the Internet, electronic bulletin board or chat room postings, user group networks, PDAs, and alpha paging units.

#### 3.6.1 **Facsimile Disclaimer Notice**

When sending a fax, especially when transmitting outside of ISO controlled machines, the cover page should contain the approved disclaimer notice at the bottom.

**Fax Disclaimer Notice:**

*This facsimile is intended only for use of the addressee(s) named herein and may contain legally privileged and/or confidential information. If you are not the intended recipient of this facsimile, you are hereby notified that any dissemination, distribution, or copying of this facsimile is strictly prohibited. If you have received this facsimile in error, please immediately notify us by telephone and return the original facsimile to us at the address below via the local postal service. We will reimburse any costs you incur in notifying us and returning the facsimile to us.*


#### 3.6.2 **Electronic Mail Disclaimer Notice**

When sending e-mail messages, the approved disclaimer notice must be used at the bottom of the message (refer to sub-section 3.8.1 when working with Legal):

**E-Mail Disclaimer Notice:**

*The foregoing e-mail communication, together with any attachments thereto, is intended for the designated recipient(s) only. Its terms are Confidential. Unauthorized use, dissemination, distribution, or reproduction of this message is strictly prohibited.*

The ISO e-mail system will automatically appended the following disclaimer notice to all external bound e-mail:

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

*The foregoing electronic message, together with any attachments thereto, is confidential and may be legally privileged against disclosure other than to the intended recipient. It is intended solely for the addressee(s) and access to the message by anyone else is unauthorized. If you are not the intended recipient of this electronic message, you are hereby notified that any dissemination, distribution, or any action taken or omitted to be taken in reliance on it is strictly prohibited and may be unlawful. If you have received this electronic message in error, please delete and immediately notify the sender of this error.*

### 3.6.3 Posting Disclaimer Notice

When posting company related messages on the Internet or other electronic bulletin boards, or when sending email messages over the Internet, the disclaimer should be used to ensure that the recipient(s) or readers do not mistakenly accept it as ISO stance, support, or endorsement. It is the sender's sole opinion.

**Posting Disclaimer Notice:**

*The foregoing e-mail communication (together with any attachments thereto) represents my personal opinions and not an official endorsement by or a position supported by the California ISO, my current employer. I reserve the right to disavow them at my convenience.*

## 3.7 Distribution of ISO Operating Procedures


The ISO currently publishes most of its Operating Procedures on the ISO Home Page. However, there are several ISO Operating Procedures ("IOP"s) that are not released to the general public as they contain information that is either confidential, proprietary or would otherwise jeopardize the grid security.

This standard coding of Operating Procedures addresses the fact that while every effort is being made to make most available, certain IOPs must remain out of the public view, primarily to address the security of the grid and power system operations.

This standard coding of Operating Procedures also outlines the method for determining which IOPs are not made public, and describes the approval requirements for any limited distribution of the non-public IOPs.

### 3.7.1 Determination of Sensitivity

As of October 4, 2000, a one-letter code will be assigned to each of the sensitive IOPs (indicated in the title block of the IOP) by the ISO Legal & Regulatory Department, working with the Procedure Control Desk. The letter code designation indicates that the IOP cannot be distributed to non-ISO employees without first receiving approval for

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

release as described below. Any IOP *without* such a letter code will, as of October 4, 2000, be deemed available to the public and will be transferred, in due course, from the ISO's private intranet site to the ISO's public Internet Home Page.

Prior to October 4, 2000, an IOP is considered "sensitive" if it is not published on the ISO's public Internet Home Page. Consequently, ISO employees should not distribute IOPs or IOP attachments located on the intranet, to non-ISO employees unless and to the extent they have received the approval described herein. Post October 4, 2000 *if it is for distribution outside the ISO it will be on the Internet*.

### 3.7.2 Assignment of Sensitivity Codes K, S, and P

In the normal course of developing and updating IOPs, the Procedure Control Desk will propose sensitivity codes for IOPs as appropriate, to be reviewed and approved by the ISO Legal & Regulatory Department. IOPs or attachments that are coded as "K", "S" or "P" may *not* be released to the public or to any non-ISO employee without the approval of the ISO Legal and Regulatory Department.

### 3.7.3 Description of Codes K, S, and P


#### 3.7.3.1 Market Sensitivity Code K

Any IOP or attachment that contains information that could harm competitive markets or a Market Participant including, but not limited to:

- Naming of specific generating units and their ratings or required operating levels;
- References to increasing or decreasing the output of specific generating plants;
- Naming specific curtailable loads and their ratings or required operating levels;
- Start-up, fixed cost, or production cost data, or currently applicable operating characteristics or statistics specific to generating plants, specific generating units or curtailable loads;
- Setting out specific effectiveness factors for facilities.

#### 3.7.3.2 System Security Code S

Any IOP or attachment that contains information that could be used by any public party to threaten or jeopardize:

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

- (1) The security of personnel operating the ISO Control Area and internal power systems;
- (2) The reliable operation of the ISO Control Area; or
- (3) The security of the ISO Controlled Grid, including, but not limited to:
  - Naming specific ISO or Operating Company personnel;
  - Names, addresses, phone numbers, e-mail addresses, and the like, of operations personnel at the ISO or at other operating companies (e.g., generators, transmission owners, other control area operators, etc.);
  - Naming of specific facilities that can be operated to connect or disconnect generators, loads, or other power system equipment (e.g. breaker numbers, switch numbers, tower no: substation, power plant or power house names, etc.).

### 3.7.3.3 Proprietary Code P


Any proprietary items, i.e., information owned by specific parties and provided to the ISO for its use including, but not limited to:

- Utility Distribution Companies' operating procedures, system one-line diagrams, switching diagrams, or operating instructions;
- Participating Transmission Owner's operating procedures, system one-line diagrams, switching diagrams, or operating instructions;
- Non-Participating Transmission Owners' (i.e., municipal, state or federal operating entities) operating procedures, system one-line diagrams, switching diagrams, or operating instructions;
- Participating Generators' operating procedures, system one-line diagrams, switching diagrams, or operating instructions;
- Operational data or operational study results.

**Note:** this standard coding of Operating Procedures is not intended to limit such information exchange, either written or verbal, between reliability entities within the WSCC Interconnection, as are necessary to conduct day to day business or during emergency situations.

## 3.8 Attorney-Client Communications

In addition to properly classifying and marking information, documented communications between an employee and a legal representative may require an additional marking further restricting use and increasing its protection. Communicating with an internal or an outside legal Counsel regarding sensitive information may require an additional notice indicating restrictive controls, as well as legal protection from disclosure.

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

### 3.8.1 Approved Notice

*Privileged and Confidential, Attorney/Client Communications.*

This will help maintain communication privileges. Not every document will require this notice. If you are not sure if you need this notice, please ask the legal representative you are working with for guidance.

### 3.8.2 Notice Format

The notice must adhere to the following format:

- The notice must be placed at the top-center of the front page (may use the *header* feature in most word-processors).
- Use a larger font size (2 or 4 points larger than the rest of the document).

### 3.8.3 Proper Use

Information communicated to and from Counsel, concerning legal advice or responding to Counsel's inquiries, requiring the notice must also be classified as CAISO Restricted and marked appropriately. Such information must be restricted to the person being communicated with and other persons identified by Counsel.


## 3.9 Intellectual Property

ISO intellectual property includes, but is not limited to all work performed by ISO personnel as part of their job function, unless stipulated differently in an approved signed contract. For example, documents, code, presentations, and reports regarding ISO and the Electric Market, in whatever medium, are considered intellectual properties of ISO. As such, all rights associated with owning it belongs to ISO.

Some of the intellectual properties may require additional legal safeguards to protect ISO interests and investments. Some of these legal safeguards include copyrights, trademarks, and patents. For more information on intellectual property and when and how to obtain these safeguards, please refer to our Legal Department.

### 3.9.1 Copyright Marking

Copyright protects ideas, thoughts, plans, and any tangible or intangible concepts that are combined and prepared (in any medium) uniquely for ISO, under ISO's authority. For more information on copyrights, please contact our Legal Department.

	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

### 3.9.2 Trademarks

A trademark is a globally recognized legal designation protecting a name or graphic (a symbol representing someone or something) so others may not take advantage and either profit from it, or cause harm to the actual owner. For more information regarding trademarks, please refer to our Legal Department.

### 3.9.3 Patents

A patent is a globally recognized legal designation protecting the ownership and all rights associated with that ownership of a tangible item (e.g., mechanical device, process, recipe, formula, etc.) that was uniquely created or developed. For more information regarding patents, please refer to our Legal Department.

## 3.10 Declassifying Information


Information sensitivity normally declines in time. When the information loses its sensitivity, the downgrading of classification must take place in a reasonable time frame. The author must reprint material with the new classification and replace the outdated version copies. All copies of the previously classified information must be disposed of as outlined in this document. The steward or designee must contact all registered holders of that document; retrieves all distributed copies, and provide declassified copies. When declassifying information, the owner must document the following:

- The date and time of change.
- Classification change (example, From CAISO Restricted to CAISO Internal Use).
- Reason for change.
- Copy of notifications sent, including:
  - Date
  - Distribution list
  - Resolution of previous copies (request old versions to be returned or destroyed)

## 4. INCIDENT REPORTING

### 4.1 General Security Breaches

It is the responsibility of all California ISO personnel aware of an actual or suspected information security breach, as defined below, to report it immediately to their respective manager and the

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

Information Security Department for review. A “security breach” means an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of information maintained by California ISO and covered under this policy. This includes physical security as well as computer or information systems security breaches that involve information assets.

In the case of a computer security breach, the Information Security Department must be notified immediately. At the direction of General Counsel, the Information Security Department will conduct an investigation of the actual or suspected breach as well as review internal procedures and controls. The Information Security Department will notify and coordinate with the senior management of the impacted department or business unit, as necessary and appropriate, to conduct the investigation.

A final report of the findings will be forwarded to the Office of General Counsel. The Information Security Department, in consultation with the Officer of General Counsel, shall make recommendations to the appropriate senior manager for review and implementation and assist in implementation of such recommendations, as appropriate. Impacted departments or business units are required to implement the corrective action agreed to by the senior manager to improve departmental controls over information security.


Departments or units will not conduct their own investigation without first consulting with the Information Security Department.

## 4.2 Computer Security Breaches

State law requires California ISO to notify any California resident for whom the ISO maintains “Personal Information” as defined in Section 3.1 of this policy, of any computer security breach that allowed an unauthorized person to acquire such resident’s information. The notice requirement is triggered if: (1) there is a breach of the security of California ISO computer system containing such personal information; (2) California ISO becomes aware of such breach; and (3) California ISO believes that an unauthorized person has acquired the personal information. This state law notification requirement only applies to computer or electronic security breaches and not to other breaches, such as incidents involving physical security.

The Information Security Department will coordinate with the Executive Director of Human Resources, the Office of General Counsel and any other relevant business unit to provide the notification required under state law. Notification to affected individuals may not occur without prior consultation and approval from the Information Security Department.

In the case of a computer security breach, the Information Security Department must be notified immediately. At the direction of General Counsel, the Information Security Department will conduct an investigation of the actual or suspected breach as well as review internal procedures and controls. The Information Security Department will notify and coordinate activities with the Chief Information Officer and Vice President of Information Services. Additionally, the

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
		<b>Information Classification Standards          And Protection Procedures</b>	
		Review By	06/21/12

Information Security Department may notify and coordinate with the senior management of the impacted department or business unit, as necessary and appropriate, to conduct the investigation.

## 5. CHANGES AND MODIFICATIONS


Suggestions to modify this information security standard must be submitted in writing to the Information Security Department for review and consideration. Each suggestion must include a business case that includes at a minimum:

- A description of the business or technological reason for modifying this document;
- A detailed explanation of the benefits the proposed suggestion can bring to the ISO; and
- An outline detailing alternative considerations.

## 6. COMPLIANCE

All personnel must comply with this standard. Compliance with this standard shall be monitored annually in conjunction with the organization's monitoring of its information security program. The Information Security Department will conduct periodic internal assessments to ensure compliance with federal and state laws and regulations as well as this policy.

California ISO personnel who do not comply with the terms of these policies are subject to disciplinary action up to and including immediate termination of employment. Consultants and contractors will be subject to termination of their contracts or requests to remove the individual offender from the California 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 California ISO will report to the appropriate authorities.

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date 06/01/10
	<b>Information Classification Standards          And Protection Procedures</b>	Version 2.9 Review By 06/21/12

## Appendix A - Classification Levels and Protection Measures

### Classification Levels

Official Marking	“CAISO Public”	“CAISO Internal Use”	“CAISO Confidential”	“CAISO Restricted”	“PCII” or “CEII”
Definition	Public information is information that can be disclosed public without restrictions in compliance with federal and state laws, and regulatory tariffs and protocols. Knowledge of this information does not violate an individual’s right to privacy or expose the corporation to financial loss, embarrassment, or jeopardize the security of assets.	Internal Use information is information that, due to technical or business sensitivity, is limited to use by employees and contractors only. Unauthorized disclosure, compromise, or destruction would not have a significant impact on the corporation or its employees.	Confidential information is information that the corporation and its employees have a legal, regulatory, or social obligation to protect. It is intended for use solely by employees who have a need-to-know. Unauthorized disclosure, compromise, or destruction would adversely impact the corporation or its employees.	Restricted information, the highest level of classification, is information whose unauthorized disclosure, compromise, or destruction could result in severe damage, provide significant advantage to a competitor, or incur serious financial impact to the corporation or its employees. It is intended solely for restricted use within the corporation and is limited to those with an explicit, predetermined “need-to-know”.	PCII or CEII classification was established by the Federal government (e.g. DHS and FERC) to protect information relating to the nation’s Critical Infrastructure Information submitted to the government by the private sector from being release to the public sector. PCII is for information being submitted to DHS and CEII if for information being submitted to FERC.
Impact of Disclosure	If disclosed, no impact to the ISO business processes or damage to company’s public image and trust.	If disclosed, low to medium impact to the ISO business processes or damage to company’s public image and trust.	If disclosed, medium to high impact to the ISO business processes such as potential compromises or damage to the company’s public image and trust. Loss of confidence by the company’s stakeholders.	If disclosed, high to critical impact to the ISO business processes, computing and communications infrastructure, individual privacy, and compromises or damage to the company’s public image and trust. Loss of confidence by the company’s stakeholders.	If disclosed, critical impact to the reliability of the nations Electric Grid.



**Information Classification Standards  
And Protection Procedures**

<p>Examples</p>	<ul style="list-style-type: none"> <li>- Published Annual Reports</li> <li>- Press releases</li> <li>- ISO Tariff</li> <li>- Information identified by the ISO Information Availability Policy</li> </ul>	<ul style="list-style-type: none"> <li>- Employee Handbook</li> <li>- Telephone Directory</li> <li>- Organization Charts</li> <li>- Company-wide Policies and Standards</li> <li>- Procedures written at a high level with no details regarding the inner working of our computing environment and communication infrastructure.</li> </ul>	<ul style="list-style-type: none"> <li>- Customer records</li> <li>- Business plans</li> <li>- Proprietary/custom software</li> <li>- Budget information</li> <li>- Strategic Plans</li> <li>- Vendor Contracts for goods and services</li> <li>- Consulting Agreements</li> <li>- Network, Security, System, and Application designs and schematics</li> <li>- Manuals on how to operate and maintain networks, systems, and applications</li> <li>- Information not meeting the criteria of the other three classification definitions, by default, becomes confidential information</li> </ul>	<ul style="list-style-type: none"> <li>- Access codes such as password or pins</li> <li>- Encryption keys</li> <li>- Market forecasts</li> <li>- Employee records including medical, financial, payroll, etc.</li> <li>- Scheduling Coordinators credit and financial records</li> <li>- Litigation documents as determined by Legal</li> <li>- Investigation reports as determined by InfoSec</li> <li>- Methodologies used by DMA</li> </ul>	<ul style="list-style-type: none"> <li>- Critical spares list</li> <li>- Location of critical sub-stations.</li> </ul>
-----------------	---	---	---	--	--

**Handling Instructions**

<p>Labeling And Marking</p>	<p><i>Required</i></p> <p>See Section 3.4</p>	<p><i>Required</i></p> <p>See Section 3.4</p>	<p><i>Required</i></p> <p>See Section 3.4</p>	<p><i>Required</i></p> <p>See Section 3.4</p>	<p><i>Required</i></p> <p>See Section 3.4</p>
<p>Reproduction</p>	<p>Permitted</p>	<p>Permitted</p>	<p>Restrictions</p>	<p>Restrictions</p>	<p>Restrictions</p>



**Information Classification Standards  
And Protection Procedures**

			Limitations: control statements set limits.	Limitation: only by the owner or designee.	Limitation: only by the owner or designee.
Distribution	Permitted	Restrictions  Limitations: internally to ISO personnel.	Restrictions  Limitations: to ISO personnel with a need-to-know.	Restrictions  Limitations: to the fewest possible ISO personnel with a need-to-know	Restrictions  Limitations: to the fewest possible ISO personnel with a need-to-know
Standard Mail Service	Permitted	Permitted	Restrictions  Limitations: regular mail mark envelope with "To Be Opened By Addressee Only".	Restrictions  Limitations: double-enveloped for internal & external mail; use express courier, registered mail, & mark outside envelope with "To Be Opened By Addressee Only".	Restrictions  Limitations: double-enveloped for internal & external mail; use express courier, registered mail, & mark outside envelope with "To Be Opened By Addressee Only".
Electronic Mail	Permitted	Permitted  Note: Use "Disclaimer" statement in Section 3.6. Remember that email is not private!	Restrictions  Limitations: Use "Disclaimer" statement in Section 3.6. Encrypt message when possible. When composing the msg., select Options-Sensitivity-Confidential to ensure msg. integrity. Remember that email is not private!	Restrictions  Limitations: Use "Disclaimer" statement in Section 3.6. Must encrypt message. Also, select Options Sensitivity-Confidential.	Restrictions  Limitations: Use "Disclaimer" statement in Section 3.6. Must encrypt message. Also, select Options Sensitivity-Confidential.
Data Transmission	Permitted	Permitted	Restrictions  Limitations: encrypt data when transmitted over external networks.	Restrictions  Limitations: encrypt data when transmitted over external networks.	Restrictions  Limitations: encrypt data when transmitted over external networks.
Facsimile (Fax)	Permitted	Restrictions  Limitations: Use	Restrictions  Limitations: Use "Disclaimer"	Restrictions  Limitations: Use	Restrictions  Limitations: Use



**California ISO**  
Shaping a Renewed Future

Corporate Standards and  
Guidelines  
Information Security

Effective Date

06/01/10

**Information Classification Standards  
And Protection Procedures**

Version

2.9

Review By


06/21/12

		“Disclaimer” statement in Section 3.6.	statement in Section 3.6. Must use ISO controlled or “trusted” fax machine. Recipient must attend receiving fax machine.	“Disclaimer” statement in Section 3.6. Must use ISO controlled or “trusted” fax machine. Recipient must attend receiving fax machine.	“Disclaimer” statement in Section 3.6. Must use ISO controlled or “trusted” fax machine. Recipient must attend receiving fax machine.
Telephone	Permitted	Permitted	Permitted	Permitted	Permitted
Cellular (Mobile) Telephone	Permitted	Restrictions  Limitations: to ISO personnel and other individuals with a need-to-know. Be aware of your surroundings.	Restrictions  Limitations: to ISO personnel and other individuals with a need-to-know. Be aware of your surroundings.	Restrictions  Limitations: use landlines only. Restrict calls to those with a need-to-know. Be aware of your surroundings.	Restrictions  Limitations: use landlines only. Restrict calls to those with a need-to-know. Be aware of your surroundings.
Internet	Permitted	Restrictions  Limitations: Access to information must be controlled and recorded.	Restrictions  Limitations: information must be encrypted and access controlled and recorded.	Prohibited	Prohibited
Intranet	Permitted	Permitted	Restrictions  Limitations: Access to information must be controlled and recorded.	Restrictions  Limitations: information must be encrypted and access controlled and recorded.	Restrictions  Limitations: information must be encrypted and access controlled and recorded.
Portable Devices	Permitted	Restrictions  Limitations: to ISO personnel and other individuals with a need-to-know. Be aware of your surroundings.	Restrictions  Limitations: to ISO personnel and other individuals with a need-to-know. Use encryption and strong authentication measures. Be aware of your surroundings.	Restrictions  Limitations: to ISO personnel and other individuals with a need-to-know. Use encryption and strong authentication measures. Be aware of your surroundings.	Restrictions  Limitations: to ISO personnel and other individuals with a need-to-know. Use encryption and strong authentication measures. Be aware of your surroundings.
Printing	Permitted	Restrictions	Restrictions	Restrictions	Restrictions



**Information Classification Standards  
And Protection Procedures**

		Limitations: User must be present while printing and remove print out immediately when using non-ISO controlled printers.	Limitations: User must be present while printing and remove print out immediately when using non-ISO controlled printers.	Limitations: must print to a local printer. If shared printer used, must be present while printing and removed immediately. Do not use non-ISO controlled printers.	Limitations: must print to a local printer. If shared printer used, must be present while printing and removed immediately. Do not use non-ISO controlled printers.
Storage	Permitted	Permitted	Restrictions Place hardcopies, diskettes, CDs, tapes in physically locked locations (e.g., in drawers and cabinets). Use access control software for hard drive storage	Restrictions Encrypt electronically stored information on desktops and laptops. Place hardcopies, diskettes, CDs, tapes in locked enclosures (e.g., drawers, cabinets or safes when not in use). User controls access to locked enclosure. Use access control software for hard drive storage on desktops and laptops	Restrictions Encrypt electronically stored information on desktops and laptops. Place hardcopies, diskettes, CDs, tapes in locked enclosures (e.g., drawers, cabinets or safes when not in use). User controls access to locked enclosure. Use access control software for hard drive storage on desktops and laptops
Destruction Any destruction must be consistent with the <u>ISO Record Retention Policy</u>	Permitted	Restrictions Hardcopies shall use Confidential Paper Shredding Receptacles.  Irretrievably erase information on hard drives, disks, tapes, or CDs, overwrite with a random pattern to meet DoD standards or physically destroy them.	Restrictions Hardcopies shall use Confidential Paper Shredding Receptacles.  Irretrievably erase information on hard drives, disks, tapes, or CDs, overwrite with a random pattern to meet DoD standards or physically destroy them.	Restrictions Hardcopies shall use Confidential Paper Shredding Receptacles.  Irretrievably erase information on hard drives, disks, tapes, or CDs, overwrite with a random pattern to meet DoD standards or physically destroy them.	Restrictions Hardcopies shall use Confidential Paper Shredding Receptacles.  Irretrievably erase information on hard drives, disks, tapes, or CDs, overwrite with a random pattern to meet DoD standards or physically destroy them.

 <b>California ISO</b> Shaping a Renewed Future	Corporate Standards and Guidelines Information Security	Effective Date	06/01/10
<b>Information Classification Standards          And Protection Procedures</b>	Version	2.9	
	Review By	06/21/12	

## Appendix B - Department Abbreviation Codes

To form the originator/author identification for a document, use the initials of each department name (starting at the top level of the org chart excluding titles such as VP or Director) and work down to your department. Place a / (forward slash) between department initials and add your name as the author at the end (e.g. AB/CDE/<author>). If there is already an abbreviation in the department name (e.g. IT), include it in the abbreviation code.

For example, the originator/author identification for Tim Lockwood in "Technology/IT Operations/Data Center & Operations" becomes "T/ITO/DCO/Tim Lockwood". Reference the [current organizational chart](#) to create your department abbreviation code.