



California ISO

Shaping a Renewed Future

Enterprise Information Security Policy Version #4.0

Effective 5/10/2012

Copyright 2012 © by California ISO.
All Rights Reserved.

REVISION HISTORY

VERSION NO.	DATE	SUGGESTED NEXT REVIEW DATE	REVISED BY	DESCRIPTION
1.0	03/10/1998	-	Aldo Nevare	Policy Adopted
2.0	10/24/2000	-	Aldo Nevare	Minor changes and reformatting, re-released.
2.1	11/06/2001	-	Aldo Nevare	Minor changes to reflect reorganization and reformatted, re-released.
2.2	02/14/2002	-	Aldo Nevare	Minor format changes by ISS.
2.3	10/09/2002	-	Aldo Nevare	Minor upgrades by ISS reflecting changes in waiver procedure.
2.4	02/13/2003	-	Aldo Nevare	Minor update to include wireless technology.
2.5	11/11/2003	-	Aldo Nevare	Minor title change and replaced CAISO acronym.
2.6	02/05/2004	-	John Gibb	Minor Format Changes, Removed Hyperlinks.
2.7	03/04/2005	-	John Gibb	Change in doc reference and compliance and consolidated repeated sections.
2.8	03/28/2005	-	John Gibb	Major rewrite
2.9	8/29/2005	-	John Gibb	Aligned signature line with procedure
2.10	9/21/2006	-	John Gibb	Updated to reflect other document changes and roles and responsibilities.
2.11	06/13/2007	-	Tim Lockwood	Classification changed to CAISO PUBLIC. Updated organizational information for originator identification.
3.0	06/04/2008	-	Tim Lockwood	Changed to new numbering scheme and added "branch" framework.
3.0	05/27/2009	-	Tim Lockwood	Reviewed, no changes required.
3.1	6/24/2009	-	Tim Lockwood	Renamed to Enterprise Information Security Policy. Deprecating the ISEC-P designation.
3.2	7/30/2009	-	Tim Lockwood	Updated roles and responsibilities.
3.3	10/15/2010	-	Tim Lockwood	Update of roles and responsibilities. Updated footer based on organizational change.
3.4	08/22/2011	-	Tim Lockwood	Updated logo and footer based on organizational change. Updated guiding principles section. Updated examples of information resources. Updated Information Security Programs to include partnership with primary owners. Updated signature block to reflect new CEO.

4.0	3/16/2012	3/16/2013	Tim Lockwood	Reviewed policy in its entirety; updated to meet new template standards
-----	-----------	-----------	-----------------	---

TABLE OF CONTENTS

1.0	INTRODUCTION	1
2.0	INFORMATION SECURITY PROGRAM	1
2.1	Guiding Principles	2
3.0	SCOPE	3
4.0	DEFINITIONS	3
5.0	ROLES AND RESPONSIBILITIES	4
5.1	All Users	5
5.2	All Officers and Managers	5
5.3	Vice President of Technology	5
5.4	Director of IT Operations	5
5.5	Manager of Information Security	5
5.6	Information Technology Managers	5
6.0	ROLES AND RESPONSIBILITIES FOR EXCEPTIONS	6
6.1	Vice President of Technology	6
6.2	Manager of Information Security	6
6.3	All Officers and Managers	6
7.0	IMPORTANCE OF COMPLIANCE	6
7.1	Maintaining Public Trust	6
7.2	Continuing Business Operations	6
7.3	Protecting ISO Investment	6
7.4	Abiding by Federal and State Regulations	7
8.0	COMMUNICATION AND TRAINING	7
8.1	Scope	7
8.2	Frequency	7
9.0	COMPLIANCE	7
9.1	Disciplinary Guidelines	7
10.0	RESOURCES AND RELATED POLICIES	7
11.0	CONTACTS	8
12.0	APPROVAL SIGNATURES	8

1.0 INTRODUCTION

This document establishes the framework for all California Independent System Operator Corporation (ISO) information security policies and standards. The ISO is committed to creating and maintaining an environment that protects information resources from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Adherence to information security policies will safeguard the integrity, confidentiality, and availability of ISO information, regardless of media type, and will protect the interests of the ISO, its personnel, its market participants and the general public.

Information security controls are intended to protect ISO information resources. Adherence to the policies is mandatory. Attempts to circumvent, subvert, remove or otherwise modify any ISO information security control for the purpose of bypassing, avoiding, or defeating any filtering, monitoring or other security controls are strictly prohibited.

Unique business requirements may require minor deviations from this policy or other related information security policies; however, all policies, standards, procedures, guidelines and practices pertaining to information security must be coordinated through Information Security.

The intent of this document is to ensure the creation and implementation of an environment that:

- Protects information resources critical to the ISO
- Protects information resources as mandated by federal and state laws
- Protects the personal information and privacy of employees and customers
- Complies with NERC CIP Standards 002-009 and the ISO NERC Tariff
- Reinforces the reputation of the ISO as an institution deserving of public trust
- Complies with due diligence standards for the protection of information resources
- Assigns responsibilities to relevant ISO executives, managers, employees, contractors, partners, and vendors

2.0 INFORMATION SECURITY PROGRAM

This document institutes controls and standard security policy elements across the corporation. Management of the information security program and the title of Manager of Information Security have been delegated to the Manager of Data Center & Operations by the President and CEO and the Vice President of Technology.

The Manager of Information Security directs the ISO information security program, which consist of the areas listed below:

- Information Security Policies, Standards, and Procedures Management
- Information Security Compliance
- Information Security Risk and Assessments Management

- Information Security Awareness and Training Management
- Information Security Incident Management
- Information Security Vulnerability Management

The Manager of Information Security also works in partnership with the sub-programs listed below:

- Regulatory Compliance Management
- Information Security Identity and Authorization Management
- Information Security Architecture Management

2.1 Guiding Principles

Information security is:

- A cornerstone to maintaining public trust.
- A business enabler – not a technology issue.
- Risk-based and cost-effective.
- Aligned with ISO priorities, industry-prudent practices, and regulatory requirements.
- Directed by policy but implemented by business owners.
- Everybody's business.

At the ISO, information is a critical and valuable asset that must be protected. The following principles guide the development and implementation of ISO information security policies and practices:

- **Complete Mediation** - This principle asserts every access to every object must be authorized.
- **Default to Deny All** - When configuring computers and communications systems make certain that the default settings are to prohibit access or functionality. Only explicitly approved services should be available and only explicitly approved systems and users should be using those services.
- **Defense-in-Depth** - To prevent single points of failure in security, when configuring computers and communications systems security controls, make certain they are deployed in a manner that is coordinated with overlapping functions. The use of multiple controls is the best way to protect the confidentiality, integrity and availability of the information assets.
- **Economy of Mechanism** - This principle asserts services and operations should be uncomplicated. This principle means “keep it as simple as possible to do the work needed.”
- **Least Privilege** - This principle asserts that a service or operator shall be granted only the permissions needed to perform a task.
- **Open Design** - This principle asserts that the security of a service or operation should not depend on the secrecy of its design or implementation.
- **Separation of Duties** - This principle asserts that for a particular set of transactions, no single service or operator be allowed to execute all transactions within the set. For example, the requestor of a transaction should not be the approver of the transaction.

3.0 SCOPE

Information security policies apply to all information in any form, related to ISO business activities, employees, or market participants, which have been created, acquired, or disseminated using ISO resources, brand or funding. These policies also apply to all technologies associated with the creation, collection, processing, storage, transmission, analysis and disposal of information and, all information systems, infrastructure, applications, products, services, telecommunications networks, and related resources, which are sponsored by, operated on behalf of, or developed for the benefit of the ISO.

Information security policies apply to all ISO functional organizations, employees, consultants, contractors, vendors, and any other authorized users of ISO information systems, applications, telecommunication networks, data and related resources conducting business with the ISO.

4.0 DEFINITIONS

Information Assurance - The practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

Information Resources - For the purposes of these policies, information technologies and the information they contain are collectively known as information resources.

Examples of Information Resources

Category	Description	Examples	
Systems and equipment	All multi-user computers and computer-controlled systems and their components	<ul style="list-style-type: none"> Data processing equipment Automated information systems (AIS) Process control computers Process control systems Embedded computer systems Minicomputers Microcomputers 	<ul style="list-style-type: none"> Microprocessors Office automation systems Stand-alone, shared logic, or shared resource systems Firmware Servers Kiosks
Single-User Computer Equipment	All computers and their components used by individuals	<ul style="list-style-type: none"> Personal computers (PCs) Workstations Laptop computers Notebooks computers 	<ul style="list-style-type: none"> Personal digital assistants Handheld computers
Hardware	All major items of equipment or their components associated with a computer system	<ul style="list-style-type: none"> Central processing units (CPUs) Terminals Monitors Speakers 	<ul style="list-style-type: none"> Video display terminals Projection equipment Modems Printers

Software	All programs, scripts, applications, operating systems, HTML, and related resources	<ul style="list-style-type: none"> • Operating systems • Programs • Applications • Applets 	<ul style="list-style-type: none"> • Database management systems • Custom code • Associated documentation
Data and Information	All information or data stored in digital format, or as a printed product of data stored in digital format	<ul style="list-style-type: none"> • Text files • Documents • Spreadsheets • Digital images 	<ul style="list-style-type: none"> • Electronic messages (e-mail, text, Instant Messages, etc.) • Tables • Databases • Biometrics information
Products and services	All objects, processes, functions, and information delivered by, for, or under the brand of the ISO	<ul style="list-style-type: none"> • Information delivery services • E-commerce applications 	<ul style="list-style-type: none"> • Digital certificate services • Website content
Network facilities	All communications lines and associated interconnected communications equipment	<ul style="list-style-type: none"> • Terminal equipment • Routers • Firewalls • Hubs • Switches • Local Area Networks (LANs) • Wide Area Networks (WANs) • Virtual Private Networks (VPNs) • Infrastructure 	<ul style="list-style-type: none"> • Internet • Intranet • Extranet • Telephones and telephone systems • Voice-messaging systems • Fax machines • Videoconferencing equipment • Wireless communications
Media	All electronic and non-electronic media used for information exchange	<ul style="list-style-type: none"> • Magnetic tapes • Magnetic or optical disks 	<ul style="list-style-type: none"> • Removable media • Hard-copy printouts

5.0 ROLES AND RESPONSIBILITIES

Information security is the individual and collective responsibility of all ISO personnel, business partners, and other authorized users. Security-related roles and responsibilities must be identified and separation of duties and responsibilities considered when defining roles. Access to information resources will be based on the individual's roles and responsibilities. Only authorized personnel will be approved for access to ISO information resources.

5.1 All Users

All ISO personnel, including employees, consultants, subcontractors, business partners, and customers who access non-public ISO information resources and other authorized users of ISO information resources are responsible for complying with all ISO information security policies.

5.2 All Officers and Managers

All officers, directors and managers, regardless of functional area, are responsible for implementing information security policies and ensuring compliance with information security policies. They provide the personnel, financial and physical resources required to determine information sensitivity and appropriately protect information resources.

5.3 Vice President of Technology

The Vice President of Technology is responsible for ensuring the secure implementation of the information technology infrastructure and has delegated authority for development, implementation and management of the ISO information security program to the Director of IT Operations. The Vice President is also responsible for information assurance.

5.4 Director of IT Operations

The Director of IT Operations is responsible for implementing a secure information technology infrastructure and development, implementation and management of the ISO information security program through the Manager of Information Security.

5.5 Manager of Information Security

The Manager of Information Security is responsible for setting the strategic direction and implementation of the information security program including the development of information security policies, standards and processes. The Manager serves as the central point of contact for all information security issues including the authority to conduct investigations of actual or suspected cyber security incidents.

The Manager of Information Security provides consultation on information security policies, standards, processes, requirements, controls, services and security awareness training. The Manager reviews compliance with information security policies through risk assessments.

5.6 Information Technology Managers

All Information Technology Managers are responsible for securing the ISO computing environment, which includes information resources and infrastructure, by implementing appropriate technical and operational security processes and practices that comply with ISO information security policies and standards.

6.0 ROLES AND RESPONSIBILITIES FOR EXCEPTIONS

Instances where the ISO cannot conform to information security policies will be documented by Information Security as an “exception”. All exceptions to information security policies and standards must be documented, approved and reviewed annually as per the *Corporate Exception to Policy Procedure*.

6.1 Vice President of Technology

The Vice President of Technology is responsible authorizing and reviewing annually all exceptions to policy.

6.2 Manager of Information Security

The Manager of Information Security is responsible for developing, facilitating, and managing all “exception” to security processes (e.g. policy and standards).

6.3 All Officers and Managers

All officers, directors and managers, regardless of functional area, must adhere to the exception process.

7.0 IMPORTANCE OF COMPLIANCE

7.1 Maintaining Public Trust

The public entrusts the ISO with information to maintain economic and operational stability of the California power grid every day – information that the ISO is required by law and good business practice to protect. Compliance with information security policies will help protect information resources and enhance the reputation of the ISO as deserving of public trust.

7.2 Continuing Business Operations

The ISO is committed to delivering superior customer service through the effective use of technology, information and automation. Compliance with information security policies will help ensure the continuous availability and integrity of the technological infrastructure that is critical to the ISO’s ability to perform its mission.

7.3 Protecting ISO Investment

ISO information resources represent a sizable financial investment in technology and information. These information resources are of paramount importance to the mission of the ISO and to the nation and must be protected.

7.4 Abiding by Federal and State Regulations

ISO information security policies are designed to respond to the letter, intent and spirit of federal and state regulations and directives.

8.0 COMMUNICATION AND TRAINING

8.1 Scope

Substantive changes to this policy will be communicated to all users via e-mail and posted electronically on eCurrent.

8.2 Frequency

Training will occur as part of the onboarding process and the annual information security computer based training.

9.0 COMPLIANCE

All affected ISO personnel must comply with this policy. Any Business Unit Manager or Director who strongly believes there is a valid technological or compelling business reason for non-compliance with this policy, in part or in its entirety, must follow the *Corporate Exception to Policy Procedure*.

9.1 Disciplinary Guidelines

In accordance with the ISO Disciplinary Guidelines, discipline for a violation of this policy is the responsibility of management in coordination with human resources, who should seek legal advice from the office of the general counsel.

10.0 RESOURCES AND RELATED POLICIES

Below is a list of additional resources, policies and procedures that are relevant to this policy. This list may be amended, revised and supplemented over time.

- [Corporate Access Control Policy](#)
- [Acceptable Use of Systems Policy](#)
- [Corporate Information Security Standards](#)
- [Information Classification Standards and Protection Procedures](#)
- [Corporate Exception to Policy Procedure](#)
- [Disciplinary Guidelines](#)

11.0 CONTACTS

For questions regarding subject matter covered in this policy, please contact Tim Lockwood.

12.0 APPROVAL SIGNATURES

This policy has been reviewed and approved by the following managers:

Responsible Manager:

Robert Melis	Signature on file	3/28/2012
Name	Signature	Date

Sponsoring Officer:

Petar Ristanovic	Signature on file	4/18/2012
Name	Signature	Date

Corporate Secretary:

Nancy Saracino	Signature on file	4/20/2012
Name	Signature	Date

President & CEO:

Steve Berberich	Signature on file	5/10/2012
Name	Signature	Date

Review Checklist

Policy Development Subject Matter Expert

Name: Meghan Roberts

Provided review of content to ensure that the policy is consistent with other referenced and related policy documents. Also assisted with use of new template and formatting.

Review 1	Review 2	Review 3
Date: 3/16/12	Date:	Date:
<input checked="" type="checkbox"/> No changes	<input type="checkbox"/> No changes	<input type="checkbox"/> No changes
<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes
<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes

Subject Matter Expert

Name: Tim Lockwood

The SME must review the policy to ensure that the policy is thorough and accurate, as well as aligned with best practices, current rules and regulations, and the current business environment.

Review 1	Review 2	Review 3
Date: 3/16/12	Date:	Date:
<input checked="" type="checkbox"/> No changes	<input type="checkbox"/> No changes	<input type="checkbox"/> No changes
<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes
<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes

Responsible Manager

Name: Robert Melis

Considered to be the owner of the policy. The manager is responsible for reviewing the policy to ensure that it is thorough and accurate, as well as aligned with best practices, current rules and regulations, and the current business environment.

Review 1	Review 2	Review 3
Date: 3-28-12	Date:	Date:
<input checked="" type="checkbox"/> No changes	<input type="checkbox"/> No changes	<input type="checkbox"/> No changes
<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes
<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes

Legal

Name: Greg Fisher

The appropriate attorney liaison from the legal department shall provide advice for the creation or review of any policy.

Review 1	Review 2	Review 3
Date: 3-20-12	Date:	Date:
<input type="checkbox"/> No changes	<input type="checkbox"/> No changes	<input type="checkbox"/> No changes
<input checked="" type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes
<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes

Corporate Compliance

Name: Lisa Milanes/Rich Vine

Responsible for reviewing new policies to determine whether ongoing policy monitoring is appropriate.		
Review 1	Review 2	Review 3
Date: 3/20/12	Date:	Date:
<input checked="" type="checkbox"/> No changes	<input type="checkbox"/> No changes	<input type="checkbox"/> No changes
<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes
<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes

Human Resources

Name: Jodi Ziemathis

Responsible for reviewing for consistency with ISO human resources and employment practices. Responsible for working with the writer to determine the appropriate method for training affected personnel, if necessary.		
Review 1	Review 2	Review 3
Date: 3/19/12	Date:	Date:
<input type="checkbox"/> No changes	<input type="checkbox"/> No changes	<input type="checkbox"/> No changes
<input checked="" type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes
<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes

Communications

Name: Stephanie McCorkle

Responsible for reviewing the policy for consistency with the ISO style guide and working with the writer to develop an appropriate method for communicating the policy to all affected personnel, if necessary.		
Review 1	Review 2	Review 3
Date: 5/7/2012	Date:	Date:
<input checked="" type="checkbox"/> No changes	<input type="checkbox"/> No changes	<input type="checkbox"/> No changes
<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes	<input type="checkbox"/> Few, non-critical changes
<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes	<input type="checkbox"/> Major changes