



California ISO
Shaping a Renewed Future

Acceptable Use of Systems Policy
Version #2.0



Effective 5/10/2012

COPYRIGHT © 2012 by California ISO.
All Rights Reserved.

REVISION HISTORY

VERSION NO.	DATE	NEXT REVIEW DATE	REVISED BY	DESCRIPTION
1.0	07/23/2002	07/23/2003	Info Security	Initial Release.
1.1	10/09/2002	10/09/2003	Info Security	Minor Changes by ISS.
1.2	06/17/2003	06/17/2004	Info Security	Minor Changes by ISS.
1.3	11/12/2003	11/12/2004	Info Security	Title change and replaced CAISO acronym.
1.4	03/03/2005	03/03/2006	Info Security	Rewrite of section 3.8 for more clarity, added section 3.12 on voice and image recording, Section 5 - added hardware, and chat & instant message subsections, general clean-up/minor changes.
1.5	08/24/2005	08/24/2006	Info Security	Update for reorganization.
1.7	06/12/2006	06/12/2007	Info Security	Updates to incorporate Instant Messaging.
1.8	06/14/2006	06/14/2007	Info Security	Updates with new logo and logo header.
1.9	06/13/2007	06/13/2008	Info Security	Classification changed to CAISO PUBLIC. Updated organizational information for originator identification.
1.9	02/07/2009	02/07/2010	Info Security	Reviewed, no changes required.
1.9	5/05/2010	5/05/2011	Info Security	Reviewed, no changes required.
1.10	10/13/2010	10/13/2011	Info Security	Updated footer based on organizational change. Revised awkward language in Section 2. Applied style guide to document. Removed reference to corporate calling cards.
1.11	01/11/2011	01/11/2012	Info Security	Copyedited and reviewed by Legal. Removed restriction on accessing external e-mail accounts. Clarified networks ISO assets are to connect to. Updated Internet services references. Removed references that may have infringed upon free speech. Added PDA and cell phone references.
2.0	03/16/2012	03/16/2013	Tim Lockwood	Updated technology references. Added specific policy for blackberry phones. Removed redundant sections. Migrated to new template. Updated reference to IS exception process. Added requirement to notify management if a device is lost or stolen.

TABLE OF CONTENTS

1.0	INTRODUCTION	1
2.0	SCOPE	1
3.0	DEFINITIONS	1
4.0	ROLES AND RESPONSIBILITIES	2
4.1	Users	2
4.2	Information Security	2
4.3	Accountability and Ownership	2
5.0	USE OF SYSTEMS	2
5.1	Personal Use	2
5.2	Harassment	3
5.3	User Identification	3
5.4	Attempts to Circumvent Security	3
5.5	Denial of Service	4
5.6	Access Rights	4
5.7	Unauthorized Access	4
5.8	E-mail and Instant Messaging	4
5.9	Internet Use	5
5.10	Telephones and Cell Phones	6
5.11	Voicemail	6
5.12	Facsimile Machines	6
5.13	Image Recording Equipment Use	7
5.14	Device Protection	7
5.15	Mobile Devices	7
5.16	Off Site Use of Systems	7
6.0	HARDWARE/SOFTWARE	8
6.1	Hardware	8
6.2	Software	8
6.3	Hostile Applications	8
7.0	SECURITY CONTROLS	9
7.1	Workstation Logical Security	9
7.2	Inactivity Measures	9
8.0	Requirements for elevated privileges	10
8.1	System Administrators	10
9.0	PRIVACY AND MONITORING USAGE	10
9.1	Privacy	10
9.2	Authorized Monitoring	11
9.3	Unauthorized Monitoring	11

10.0	INVESTIGATIONS	11
10.1	Law Enforcement Contact	11
10.2	Information Security Incident Response	11
11.0	COMMUNICATIONS AND TRAINING	12
11.1	Scope	12
11.2	Frequency.....	12
12.0	COMPLIANCE	12
12.1	Disciplinary Guidelines	12
13.0	RESOURCES AND RELATED POLICIES	12
14.0	CONTACTS.....	13
15.0	POLICY APPROVERS.....	13

1.0 INTRODUCTION

This policy provides the framework for the proper use of all California Independent System Operator Corporation (ISO) information system resources and services. It provides security measures applicable to end users, and describes behaviors that are required to maintain those measures. The policy provides effective protection for individual users, authorized access, and management of ISO information system assets and resources. This policy is a subset of the ISO umbrella policy regarding information security, the *Enterprise Information Security Policy*, and supports the *Corporate Information Security Standards*, laws, regulations, agreements, and contracts that apply to the ISO computing and networking services.

This document provides an enterprise-wide standard intended to define the acceptable use of all ISO systems. It allows for the proper use and security of all ISO computing resources, network assets, effective protection of individual users, authorized access, and proper management of those assets and resources. This policy covers information stored or transferred using computers, networks, telephones, mobile devices, and any communication device used by ISO personnel.

Use of ISO-owned equipment to access networks and computer systems is subject to ISO standards, guidelines and procedures, including state and federal laws, regulations, and tariffs. Appropriate use must be legal, ethical and within corporate expectations as described in this document and in compliance with corporate policies.

Authorized uses of ISO computing and network equipment, resources, and services must be consistent with the business mission of the ISO. Information technology equipment, resources and services include, but are not limited to, computer and communications hardware, software (third party and ISO owned) and services such as remote and Internet access.

2.0 SCOPE

This policy covers all ISO employees, consultants, contractors, vendors and market participants connecting to ISO information assets (hereafter described as “personnel” or “users”). All users who have access to ISO information technology equipment, services, systems or networks must comply with this policy and adhere to these standards.

3.0 DEFINITIONS

Users – All ISO employees, consultants, contractors, vendors and market participants who have obtained authorization to connect to or use ISO information assets.

ISO personnel – A subset of Users that includes ISO employees, consultants and contractors.

Internal Data – Data originated by the ISO.

External Data – Data originated outside the ISO for which the ISO is a custodian.

Systems – Any computer, laptop, personal digital assistant (PDA), computing resource, telephone, cellular phone, mobile device, fax equipment, telecommunication or network owned by the ISO for use by users in the execution of the ISO mission.

4.0 ROLES AND RESPONSIBILITIES

4.1 Users

Individuals that have a responsibility to maintain and care for corporate equipment assigned to them, and respect intellectual property rights, and system security mechanisms. Users of ISO systems are granted access to a wide variety of data, including internal data (e.g., financial information, personnel information, etc.) and external data. All users are required to comply with the *Corporate Information Classification Standards and Protection Procedures*.

4.2 Information Security

The team comprised of ISO personnel and resources dedicated to ensuring the security of ISO information system resources and services.

4.3 Accountability and Ownership

Information Security is responsible for creation and ongoing management of this policy.

5.0 USE OF SYSTEMS

5.1 Personal Use

ISO systems should be used for authorized company business. Personal use of these resources must be approved by local management and is limited to non-obstructive, non-offensive, and non-disruptive use. For example, placing personal reminders on Outlook Calendar, limited use of company e-mail or the telephone to communicate with family or friends, and making dinner reservations or conducting on-line banking via the Internet, etc., are acceptable. These standards and guidelines work in conjunction with the *Corporate Information Security Standards*.

Management, at its sole discretion, will determine at what point personal use of systems becomes obstructive or disruptive, or whether it affects job, system, or network performance, and will take appropriate action. Any personal use should be kept to a minimum and should not cause the ISO to incur additional costs, network risk or the need for additional resources. All information stored in, or processed on, ISO systems belongs to the ISO, and is subject to search, inspection, and seizure without notice.

Users shall not automatically forward company e-mail to an external e-mail system, since the e-mail may contain ISO confidential information.

Use of ISO systems for private commercial enterprises or personal gain is strictly prohibited.

5.2 Harassment

No user may, under any circumstance, use ISO systems to harass any other person. The ISO has adopted a zero-tolerance policy for discriminatory or harassing activities, as detailed in its *Harassment Prevention Policy* and the *Workplace Violence Prevention Policy*. The following constitutes a non-exclusive list of examples of harassment carried out over the computer or other equipment:

- intentionally using ISO information resources to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying offensive language, pictures, threats of bodily harm or other offensive materials;
- intentionally using ISO information resources to contact another person repeatedly with the intent to annoy, harass, or bother whether or not an actual message is communicated or a legitimate purpose for the communications exist, once the recipient has expressed a desire for the communications to cease;
- intentionally using ISO information resources to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, such as debt collection, once the recipient has provided reasonable notice that he or she desires such communications to cease;
- intentionally using ISO information resources to invade the privacy of or to threaten to invade of the privacy of another person.

5.3 User Identification

Computer accounts, passwords, remote access credentials and other types of identification are assigned to individual users and may not be shared with, or divulged to, others. Each user is responsible for all actions taken on the system with his or her user ID, and will be held accountable for both permitted and unauthorized use of the system attributable to the user's conduct.

Users may never use someone else's ID, with the exception of technical support personnel performing maintenance on a user's computer. If users suspect their user identification has been compromised, they shall immediately change all passwords and report the incident to Information Security.

5.4 Attempts to Circumvent Security

Users are prohibited from attempting to circumvent or subvert any security controls on ISO systems. No user may install, remove, or otherwise modify any hardware or software for the purpose of bypassing, avoiding, or defeating any filtering, monitoring, or other security controls used by the ISO.

5.5 Denial of Service

Users may not deliberately attempt to degrade the performance of ISO systems or to deprive other users of resources or access to any ISO systems.

Harmful activities are prohibited. Examples include, but are not limited to the following: IP spoofing; creating or propagating viruses; port scanning; disrupting services; damaging files; intentional destruction of, or damage to, equipment, software, and data; and loading non-authorized software on ISO systems.

5.6 Access Rights

User access rights will be provided following the Principle of Least Privilege. All personnel will follow the *Corporate Access Control Policy* to gain access to ISO computing resources.

5.7 Unauthorized Access

Users may not intentionally:

- damage ISO systems or other company equipment;
- obtain or use equipment not authorized to them;
- deprive another authorized user of access to ISO systems; or
- gain unauthorized access to systems by using knowledge of a special password, loopholes in computer security systems, another user's password, or access privileges not yet revoked due to a job change within the organization.

5.8 E-mail and Instant Messaging

E-mail and instant messaging (IM) messages are official ISO correspondence in the same standing as formal, written company memoranda. They represent the ISO. All official e-mail and IM correspondence must use the respective ISO services (e.g., e-mail and IM servers).

ISO e-mail and IM systems may not be used to engage in any illegal, improper or unethical activities. ISO e-mail and IM systems are intended for personnel only and may not be used by third parties, including customers or the general public.

When transmitting sensitive and confidential data, such as ISO trade secrets or proprietary or confidential information, Users must follow the standards set forth in the *Corporate Information Classification Standards and Protection Procedures*.

Users may not transmit for non-ISO business purposes any ISO trade secrets, proprietary or confidential information, contractual information, or any other information that could infringe on copyright laws.

Personnel may not use 'auto-forward' rules to forward any of their e-mail to personal mailboxes on non-ISO computers, since security and accountability cannot be maintained on those systems. For example, personnel may not set up a rule in their ISO mailbox that forwards all e-mail to their homes, or, for contractors, to their primary workplace. If you need to access ISO e-mail while outside the office, you may use Outlook Web Access (OWA).

E-mail and IM administrators may not browse the e-mail or IM messages of other personnel, unless such browsing is part of their written job description, function, or if directed to do so by a corporate officer or Information Security, Human Resources, or Legal departments.

5.9 Internet Use

Personnel have internet access so they can leverage the knowledge and resources available online to help them perform their jobs. The ISO provides internet access to personnel with the assumption that doing so enhances the efficiency, effectiveness and productivity of the company as a whole.

All information transferred using ISO internet access should be treated with the same standards as information on ISO letterhead. Communications going over the Internet (e.g., to newsgroups, blogs, social media) may automatically carry an ISO identifier and could be misconstrued as representing ISO policy or position. Personnel should refrain from using their ISO-issued email address for posting non ISO-approved communications over the internet. A disclaimer to the effect that the contents do not represent ISO policy should be appended to all non ISO-approved internet postings. Additional information on disclaimers can be found in the *Corporate Information Classification Standards and Protection Procedures*.

When onsite at the ISO, personnel must use ISO local area network hardware and software as the gateway to the Internet.

Internet access shall not be used to conduct excessive personal business, play computer games, gamble, run a business or conduct political campaigns. ISO personnel are also prohibited from using ISO internet access to represent their own personal opinions or biases as an ISO endorsement or position. ISO personnel may not use the ISO Internet connection to obtain inappropriate material, including but not limited to sexually explicit material, pornography, or material that may be interpreted as harassing or defamatory, or of a solicitous nature (e.g., literature related to hate crimes or other criminal activity, etc.). Further, users are prohibited from using ISO internet access to take part in any prohibited, terrorist or illegal activity.

Users may not use ISO internet access to knowingly download or distribute pirated software or data.

Personnel should be aware that when browsing the internet, each web server has access to information relating to the user, the computer that he or she is on and the other web locations that have been visited during each browsing session. Thus, users should use discretion when accessing web sites on an ISO computer.

The Information Security Department may monitor internet use periodically, during potential security incidents and, for personnel, as part of the formal or informal performance evaluation process. Any indication of potential misuse or violations will be turned over to ISO management for review and action.

Additional standards relating to internet security can be found in the *Corporate Information Security Standards*.

5.10 Telephones and Cell Phones

When using the telephone, especially a cell phone, speakerphone or public telephone, users should take care to ensure that their conversations cannot be overheard. This applies in the office and in public areas when speakers conducting ISO business can be overheard by many people.

Forwarding callers to external telephone numbers may result in toll fraud; therefore, users may not transfer, forward or "auto-forward" their ISO desk telephone number to a non-ISO external phone number without manager approval. Transfers can be made to other ISO telephone and cell phone numbers.

ISO personnel should also take care to protect voicemail access numbers from being compromised when using public telephones, cell phones or telephones with re-dial capabilities.

The leader of a conference call is responsible for ensuring only authorized individuals are connected to the call.

Cordless phones should never be used to discuss confidential ISO information. Definitions of information classifications are included in the *Corporate Information Classification Standards and Protection Procedures*.

5.11 Voicemail

Highly sensitive information should not be left as voice messages on internal or external systems. Either call the person back or leave a message asking to return your call. Information classifications are defined in the *Corporate Information Classification Standards and Protection Procedures*.

5.12 Facsimile Machines

Fax messages have the same standing as formal, written company memoranda, and they represent the ISO.

Fax messages are official ISO correspondence. ISO personnel must follow the *ISO Records Management Policy* regarding the retention and deletion of records.

For more information about faxing documents, refer to the *Corporate Information Classification Standards and Protection Procedures*.

5.13 Image Recording Equipment Use

The use of any type of equipment for the purpose of capturing any still or moving analog or digital images or sound recordings is not allowed within any of the ISO data centers without the prior approval of Information Security.

5.14 Device Protection

Users are responsible for protecting their ISO issued equipment from unauthorized access and theft at all times. Users should never leave laptops or wireless devices unattended in populated public places such as airports or subways, or in the checkrooms of hotels or restaurants.

Furthermore, laptops and wireless devices may never be checked on an airplane as baggage; they must be carried onto the aircraft. It is strongly recommended that laptops and wireless devices never be left in automobiles, as automobiles are theft-prone locations.

Users must report any lost or stolen devices to management immediately.

5.15 Mobile Devices

The authorized user of a mobile device is responsible for its physical security. Mobile devices are expected to be secured with a password.

Because of the limited threat, mobile devices do not require malware protections. Blackberry and iPad devices will be protected using the cryptographic protections present in the platform. The backups of mobile devices are the responsibility of the owner of the device. Mobile devices are allowed to be used in any area, including public locations.

5.16 Off Site Use of Systems

Users who work with ISO information in a home or other off-site locations should understand that information security also applies there. Some of the same security exposures exist in both types of locations, and additional exposures can exist in home or other external locations.

The physical security of a remote access site is the user's responsibility. Users who work at home (or elsewhere) should be aware of the security threats within their environment and take appropriate measures to ensure the proper safeguarding of the information as defined in the *Corporate Information Classification Standards and Protection Procedures*.

Unless otherwise prohibited by an employee's manager or ISO policy, any type of work activity, working hours, and access to data of any classification is permissible to remote access users. Users approved for remote access via virtual private network (VPN) connectivity must use ISO issued assets for such remote access. Remote access to email via Outlook Web Access (OWA)

or other web browser –based remote access such as Citrix Metaframe is allowed using non ISO assets.

Remote access to ISO systems is allowed via any remote network (home wireless, public wireless hotspot, commercial wireless services, etc). All employees are required to authenticate to the ISO network via the enterprise authentication mechanisms (Active directory, Safeword token, etc.) prior to accessing ISO networks.

6.0 HARDWARE/SOFTWARE

6.1 Hardware

The computing workspace provided is designed to meet the general needs of all users. If users find that they need functionality not provided in the standard hardware issued to them, they should contact ISO Support Services Service Desk with their requirements.

Users may not install personal or commercial hardware onto ISO workstations. This hardware includes, but is not limited to wireless cards and external storage devices which could be incompatible with ISO software and could create security vulnerabilities.

No user should directly connect any hardware device to the ISO LAN or workstation (e.g., USB drives, handhelds, etc.) that was not supplied by ISO Support Services or approved by their manager.

6.2 Software

The computer software and applications provided are configured to meet the general needs of all users. If users find that they need functionality not provided in the standard suite of programs, they should contact the ISO Support Services Service Desk with their requirements.

Users may not install personal or commercial software, shareware, freeware, adware, or any other software onto ISO workstations or other assets such as cell phones and PDAs. Such files could be incompatible with standard ISO software, and could create security vulnerabilities.

Users may not install or re-install any other operating system, such as Linux, onto an ISO workstation or server without approval and assistance from Systems Engineering and Administration.

6.3 Hostile Applications

Hostile applications include, but are not limited to: sniffers, password crackers, backdoor programs, Trojan horses, viruses, worms, port scanners, vulnerability scanners, war dialers and similar programs.

Users may not copy, install, or use hostile applications or systems on any ISO computer or network. In some cases these tools are useful for administrators or investigators, but must not be

used without an approved change request with permission from Information Security and the user's manager or contract manager.

7.0 SECURITY CONTROLS

7.1 Workstation Logical Security

Viruses can cause substantial damage to systems and data. All ISO workstations (e.g., laptops, desktops, etc.) must have company approved antivirus software installed, running and updated at all times. Users may not disable, prevent automated updates or scans, or reconfigure workstation updates in any way that decreases its functionality.

Files stored on workstations are not backed up, and therefore may be lost as the result of hardware failure, malicious or poorly written software, or malicious or accidental actions. Users must follow the *ISO Records Management Policy* regarding the retention and deletion of ISO records. Files for which the *Corporate Records Retention Policy* does not apply should be stored on the user's home directory on the appropriate file server.

Primary copies of sensitive ISO information may not be stored on the hard drive of any mobile computer. Such information may be stored for use during those times that the user cannot connect to the ISO network, but the information must be secured according to requirements based on the data classification level. See the *Corporate Information Security Standards* for information on classification levels. The information should be deleted from the mobile computer as soon as it is no longer needed.

7.2 Inactivity Measures

System Configuration

System configurations on time-out and log-off standards can be found in the *Corporate Information Security Standards*.

Authorized User Responsibility

Whenever users leave their workstations, even momentarily, they must lock their workstation rather than rely on screen saver timeout.

Mobile Computer Security Controls

Laptops and PDAs (e.g., BlackBerries, etc.) may never be checked-in as luggage when traveling.

Laptops must be carried with the user in a briefcase or a laptop carrying case.

Airport X-ray machines do not damage the data on laptops, PDAs or flash drives. ISO personnel are expected to cooperate with airport security personnel during the inspection of all electronic equipment and baggage.

Users should be aware that theft often occurs in the security screening area of airports, particularly at the moment when items are scanned electronically. Belongings should not be

placed onto the conveyor belt until you can immediately pass through the scanner to get your items, or until you can have an associate waiting on the other side of the scanner.

When laptops and PDAs are not being used, they should be stored in a secure fashion, out of plain view. Laptops and PDAs should never be left on the seat of a car, even in a briefcase.

8.0 REQUIREMENTS FOR ELEVATED PRIVILEGES

This section outlines the requirements placed on users who have elevated privileges on individual workstations, such as power user or administrator privileges. All users with elevated privileges are required to follow the additional requirements outlined below.

8.1 System Administrators

A system administrator may access the files of other users for the maintenance of networks, computers and storage systems, including creating backup copies of media. However, in all cases, administrators may not regularly open and peruse files, other than in accordance with these standards and guidelines. Administrators may not change security settings unless approved by change management.

System administrator privileges are granted only to those that have a demonstrated business need for the privileges. To obtain system administrator privileges, a request that includes the justification for system administrator privileges must be sent to the ISO Support Services Service Desk. If the need is justified and required approvals obtained, system administrator status will be granted to specific hosts.

When a user changes job positions or assignments, IT Operations will automatically remove system administrator privileges. If system administrator privileges are required in the new position or assignment, a new request for these privileges must be made. Managers or system owners responsible for managing shared accounts must ensure shared account passwords are changed, in the event a user with access to a shared account changes position or assignment and no longer requires access to the shared account(s).

9.0 PRIVACY AND MONITORING USAGE

9.1 Privacy

ISO computing resources are provided to users to enable them to perform their job functions. However, users should not have an expectation of absolute privacy in the materials they create, send or receive on ISO systems. To the extent permitted by local laws and regulations, ISO authorized personnel (such as Information Security team members, Information Security Incident Response Team (ISIRT) members and Information Technology support personnel) may examine all material stored on ISO systems without prior notice. Examples of situations warranting such examination may include investigation for a suspected breach of security, the prevention or detection of crime, and other legally permissible situations.

9.2 Authorized Monitoring

The *Corporate Information Security Standards* outlines management's ability to monitor use and perform periodic auditing of all equipment and software provided to all users without consent or notification. Such monitoring and auditing may occur because of the following:

- personal observation;
- complaints from another user;
- observations by an administrator during the normal performance of his or her job function or assignment;
- reports from Information Security Department employees as the result of an investigation into a security incident;
- observation from Information Security Department employees resulting from periodically performed spot checks of system usage;
- requests from Human Resources employees or the ISO Legal Department as a result of an investigation into harassment, discrimination, performance or other related issues;
- results from software, hardware and network monitoring tools; and,
- requests from local, state or federal regulatory bodies or law enforcement.

9.3 Unauthorized Monitoring

Users may not use computing resources or network analytical equipment or software to monitor electronic communications such as e-mail or IM messages of other ISO users. This is an unauthorized use of equipment or services and will be considered a security incident and investigated by the Information Security in cooperation with Human Resources and Legal.

10.0 INVESTIGATIONS

10.1 Law Enforcement Contact

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

10.2 Information Security Incident Response

All users share responsibility for intrusion detection, prevention and response, and are required to report any 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 to ensure the safety and protection of ISO resources.

In such instances, you should immediately notify:

- the Information Security department;
- your manager or contract manager; and

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

11.0 COMMUNICATIONS AND TRAINING

11.1 Scope

Any changes to this policy will be communicated to all users via e-mail.

11.2 Frequency

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

12.0 COMPLIANCE

All ISO personnel must comply with this policy and adhere to these standards, and apply the guidelines when possible. Any exceptions to this policy or these standards must follow the Information Security Exception Process.

12.1 Disciplinary Guidelines

In accordance with the ISO *Disciplinary Guidelines*, discipline for a violation of this policy is the responsibility of management in coordination with the Human Resources Department, who should seek legal advice from the Office of the General Counsel. 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.

13.0 RESOURCES AND RELATED POLICIES

Below is a list of additional resources, policies and procedures that are relevant to this policy.

- [Corporate Access Control Policy](#)
- [Corporate Information Classification Standards and Protection Procedures](#)
- [Enterprise Information Security Policy](#)
- [Corporate Information Security Standards](#)
- [Disciplinary Guidelines](#)
- [Employees Code of Conduct and Ethical Principles](#)

- [Harassment Prevention Policy](#)
- [Information Security Incident Response Team Procedure](#)
- [ISO Records Management Policy](#)
- [Workplace Violence Prevention Policy](#)

14.0 CONTACTS

For questions regarding subject matter covered in this policy, please contact the Information Security Department at InfoSecConcerns@caiso.com.

15.0 POLICY APPROVERS

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

Responsible Manager:

Robert Melis	Signature on file	3/28/2012
Manager, Data Center & Operations	Signature	Date

Sponsoring Officer:

Petar Ristanovic	Signature on file	4/18/2012
VP, Technology	Signature	Date

Corporate Secretary:

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

President and CEO:

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