


 California ISO <small>Shaping a Renewed Future</small>	Corporate Standards and Requirements Vendor Remote Access	Effective Date	11/29/2006
Vendor Remote Access Standards and Security Requirements		Version	1.1
		Review By	09/04/2010



Vendor Remote Access Standards and Security Requirements

 California ISO <small>Shaping a Renewed Future</small>	Corporate Standards and Requirements Vendor Remote Access	Effective Date 11/29/2006
	Vendor Remote Access Standards and Security Requirements	Version 1.1 Review By 09/04/2010

REVISION HISTORY

VERSION NO.	DATE	DESCRIPTION
DRAFT 0.1	06/07/2003	Initial draft for ISS review.
DRAFT 0.2	06/16/2003	Initial draft release for review.
1.0	10/28/2003	Initial Release.
1.1	11/29/2006	Changed ISS to InfoSec
1.1	05/06/2008	Reviewed, no changes required.
-	09/04/2009	Annual Review. Changed signature block to R. Melis

 California ISO <small>Shaping a Renewed Future</small>	Corporate Standards and Requirements Vendor Remote Access	Effective Date 11/29/2006
	Vendor Remote Access Standards and Security Requirements	Version 1.1 Review By 09/04/2010

TABLE OF CONTENTS

REVISION HISTORY2

1. OVERVIEW4

 1.1. PURPOSE4

 1.2. SCOPE4

2. VENDOR REMOTE ACCESS STANDARDS4

 2.1. VENDOR REMOTE ACCESS GUIDELINES5

3. REMOTE ACCESS SECURITY REQUIREMENTS5


 3.1. PROJECT SPECIFIC5

4. ROLES AND RESPONSIBILITIES5

5. COMPLIANCE.....6

6. APPROVAL6

 6.1. STANDARDS AND GUIDELINES APPROVAL6

	Corporate Standards and Requirements Vendor Remote Access	Effective Date	11/29/2006
	Vendor Remote Access Standards and Security Requirements		Version
Review By			09/04/2010

1. OVERVIEW

1.1. PURPOSE

The purpose of these corporate standards and security requirements is to provide a framework and guidelines to the California Independent System Operator (CAISO) and the vendors, which are contracted to conduct business with CAISO. Remote access by contracted vendors is a business requirement that facilitates the administration and management of that resource. This remote access must be provided in accordance with the CAISO information security policies, standards, and requirements to ensure the protection of the data and information being accessed, processed, or transmitted.

Remote access to any CAISO network, system, application or database must comply with CAISO's security program and architecture. All access, including remote access by vendors, must comply with fundamental security practices including proper identification, strong authentication and authorization, as well as adhere to data confidentiality and integrity, audit guidelines to ensure non-repudiation.

1.2. SCOPE

These corporate standards and requirements encompass all CAISO personnel and contracted vendors requiring remote access.


2. VENDOR REMOTE ACCESS STANDARDS

Vendor access to CAISO information systems either by direct connection (network) or by indirect connection (remote access such as dial, ISDN, DSL, wireless, microwave, etc.), must adhere to the control mechanisms and procedures implemented and managed by CAISO. These controls are put in place to afford proper identification, strong authentication and authorization, as well as to ensure confidentiality, integrity, non-repudiation, and audit capabilities to activities performed by all users, including vendor remote access. These controls will ensure that only authorized vendor personnel are accessing only the information they need to do their job or tasks such as technical support, code drop off or installation, upgrades or updates, and maintenance monitoring.

All vendor remote access users must comply with the CAISO Information Security Standards and Guidelines regarding strong authentication, individual IDs, strong passwords, and least privileged. They must also comply with the CAISO User Access Security Requirements and Procedures to ensure proper authorization and least privileged access. Vendor remote access users must also comply with the CAISO IT Equipment and Services Acceptable Use Policy, Standards to ensure proper use of the resources being used and accessed. They must also comply with the CAISO User Access Policy.

Audit capabilities for remote access must, at a minimum, record the following:

- Successful logins by ID, including date and time of login and log-off.
- Unsuccessful login attempts by ID, including date and time.
- Duration of login.
- Log activities and events.

	Corporate Standards and Requirements Vendor Remote Access	Effective Date	11/29/2006
	Vendor Remote Access Standards and Security Requirements		Version
Review By			09/04/2010

2.1. VENDOR REMOTE ACCESS GUIDELINES

Vendors requiring remote access should provide the CAISO Project Manager they are working with and the Information Security Department with a list of authorized personnel requiring individual IDs and passwords to remote access a network, system, application or database. In addition, the Project Manager must provide ISS with a list of CAISO personnel with the authority to authorize vendor access.

Audit capabilities should include other activities as well such as anomalies, date and time of installations or de-installs (history), and continuously maintain the list of names as frequently as personnel changes.

3. REMOTE ACCESS SECURITY REQUIREMENTS

Below are the security requirements that must be met in order to approve vendor remote access to CAISO resources:


- CAISO Project Managers must work with InfoSec to design and implement a secure method of remote access, which may include encryption, VPN, SSL, or secure tokens.
- Vendor must provide a list of personnel authorized to remote access CAISO resources. The list must be continuously updated due to personnel changes.
- Users must have individual IDs and passwords, no group IDs or passwords are allowed.
- Access restricted to only the data or information required to complete their assigned task or function and nothing else.
- Systems, applications and databases being accessed must have audit capabilities to record logins, failed logins, dates, times, duration, and system anomalies as described in the standards section of this document.
- CAISO Project Manager or designee must approve and authorize the vendor's remote access prior to that access.
- Vendor developers may access CAISO development and testing systems only.
- Vendor maintenance programmers may access production systems to technical support (e.g.: troubleshooting, update or upgrade installations).

3.1. PROJECT SPECIFIC

The project's management must consult with InfoSec to design the best method of remote access to comply with both the business requirements and security requirements. The classification of information being accessed will determine the level of security required to protect the data or information. The Project Manager, vendor and InfoSec should develop and document an authorization procedure including when the vendor can remotely access the system, and how the authorization is granted. Additional measures and practices may be required in addition to the ones listed above.

4. ROLES AND RESPONSIBILITIES

The Project Manager is responsible to ensure InfoSec is contacted when the vendor requirements include remote access. ISS and the Project Management team will discuss all requirements and develop the best method to implement secured remote access. The contracted vendor requiring remote access must justify the request and comply with all CAISO remote access standards and security requirements. Remote users must also adhere to the separation of duties, e.g.: developers

 California ISO <small>Shaping a Renewed Future</small>	Corporate Standards and Requirements Vendor Remote Access	Effective Date	11/29/2006
	Vendor Remote Access Standards and Security Requirements	Version	1.1
		Review By	09/04/2010

may access development and testing systems, maintenance programmers may access production under strict access restrictions.

5. COMPLIANCE

Employees affected by these Standards and Requirements are subject to disciplinary action for failure to comply with its terms, up to and including immediate termination of employment. Consultants and contractors affected by these Standards and Requirements will be subject to termination of their contracts or requests to remove the individual offender from the CAISO'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 CAISO will report to the appropriate authorities. Exceptions must be documented as described in the *Corporate Information Security Standards*.

6. APPROVAL

6.1. STANDARDS AND GUIDELINES APPROVAL

These Standards and Security Requirements were created under a stakeholder process including Information Security Services, Market Operations, and others. Due to the scope of these standards and guidelines, the following are the approving signatures:

Responsible Manager:

Robert Melis, Manager, Data Center and Operations	X
Print Manager's Name and Title	Telephone

Signature	Date
-----------	------