
 California ISO <i>Shaping a Renewed Future</i>	Enterprise Policy Information Security	Effective Date	11/30/2011
NERC CIP Security Policy		Version	1.6
		Review By	11/30/2012



California ISO
Shaping a Renewed Future

NERC CIP Security Policy

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

REVISION HISTORY

VERSION	DATE	DESCRIPTION
1.0	06/13/2008	Initial release.
1.1	12/18/2008	Minor grammar changes to clarify alignment of requirements to policy.
1.2	05/05/2009	Added 4-1.2, 4-1.3 Access policy statement to address emergency break/fix situation in relation to training and background check requirements.
1.2.1	5/18/2009	Added dial up access policy for Critical Cyber Assets to Section 5.1.2
1.2.2	6/16/2009	Incorporated comments from Legal and fixed grammatical errors. Deprecated ISEC-P naming convention.
1.2.3	9/10/2009	Included section for Emergency Provision. More closely aligned wording to CIP standards. Fixed minor grammatical issues. (TL)
1.3	12/21/2009	Added language that speaks to the annual application of the risk –based assessment methodology for Critical Assets. Added verbiage to cover technical feasibility exceptions process to augment policy exception language. Minor revisions per ISO style guide.
1.4	02/19/2010	Made changes to policy per CIP-002 through CIP-009 version 2 changes.
1.5	11/12/2010	Made changes to policy per CIP-002 through CIP-009 version 3 changes. Updated Senior Manager signature.
1.6	11/7/2011	Annual review of policy performed as part of external sufficiency review. Changed logo, added reference to delegate being able to approve physical security plan in section 6.1, consolidated and updated emergency provision clause along with examples in section 10, added technically feasible clause for passwords in section 7.6, referenced corporate exception to policy procedure in section 3.3.



	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	PURPOSE	5
2	CIP-002: CRITICAL CYBER ASSET IDENTIFICATION	5
2.1	ROLES AND RESPONSIBILITIES	6
2.1.1	<i>Manager of Information Security</i>	6
2.1.2	<i>Manager from Grid and Market Operations</i>	6
2.1.3	<i>Manager of Physical Security</i>	6
2.1.4	<i>Information Technology Managers</i>	6
3	CIP-003: SECURITY MANAGEMENT CONTROLS	6
3.1	CYBER SECURITY POLICY	6
3.2	LEADERSHIP	6
3.3	EXCEPTIONS	7
3.4	INFORMATION PROTECTION.....	7
3.5	ACCESS CONTROL	7
3.6	CHANGE CONTROL AND CONFIGURATION MANAGEMENT.....	8
4	CIP-004: PERSONNEL AND TRAINING.....	8
4.1	AWARENESS	8
4.2	TRAINING.....	8
4.3	PERSONNEL RISK ASSESSMENT	8
4.4	ACCESS.....	9
5	CIP-005: ELECTRONIC SECURITY PERIMETER	9
5.1	ELECTRONIC SECURITY PERIMETER	9
5.2	ELECTRONIC ACCESS CONTROLS.....	9
5.3	MONITORING ELECTRONIC ACCESS.....	9
5.4	CYBER VULNERABILITY ASSESSMENT.....	10
5.5	DOCUMENTATION REVIEW AND MAINTENANCE.....	10
6	CIP-006: PHYSICAL SECURITY.....	10
6.1	PHYSICAL SECURITY PLAN	10
6.2	PROTECTION OF PHYSICAL ACCESS CONTROL SYSTEMS	10
6.3	PROTECTION OF ELECTRONIC ACCESS CONTROL SYSTEMS	10
6.4	PHYSICAL ACCESS CONTROLS	10
6.5	MONITORING PHYSICAL ACCESS.....	11
6.6	LOGGING PHYSICAL ACCESS	11
6.7	ACCESS LOG RETENTION.....	11
6.8	MAINTENANCE AND TESTING	11
7	CIP-007: SYSTEMS SECURITY MANAGEMENT.....	11
7.1	TEST PROCEDURES	11
7.2	PORTS AND SERVICES	12
7.3	SECURITY PATCH MANAGEMENT	12
7.4	MALICIOUS SOFTWARE PREVENTION	12
7.5	ACCOUNT MANAGEMENT	12
7.6	SECURITY STATUS MONITORING	13

 California ISO <i>Shaping a Renewed Future</i>	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

7.7 DISPOSAL OR REDEPLOYMENT13

7.8 CYBER VULNERABILITY ASSESSMENT.....13

7.9 DOCUMENTATION REVIEW AND MAINTENANCE.....13

8 CIP-008: INCIDENT REPORTING & RESPONSE PLANNING13

8.1 CYBER SECURITY INCIDENT RESPONSE PLAN.....13

8.2 CYBER SECURITY INCIDENT DOCUMENTATION14

9 CIP-009: RECOVERY PLANS FOR CRITICAL CYBER ASSETS14

9.1 RECOVERY PLANS14

9.2 EXERCISES14


9.3 CHANGE CONTROL14

9.4 BACKUP AND RESTORE.....14

9.5 TESTING BACKUP MEDIA.....15

10 EMERGENCY PROVISIONS15

11 POLICY APPROVAL.....16

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

1 INTRODUCTION

This document establishes the policies governing the California Independent System Operator Corporation (ISO) responsibilities to NERC Critical Infrastructure Protection (CIP) Standards 002-009.

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 interest 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 for all ISO employees, contractors and vendors. The ISO strictly prohibits 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.

1.1 PURPOSE


This document is designed to institute controls and standardize security policy elements across the entire company as they relate to NERC standards and critical assets (CAs) and critical cyber assets (CCAs). The intent of this document is to create and implement an environment that:

- a. Protects information resources critical to the ISO, and
- b. Complies with NERC CIP Standards 002-009.

2 CIP-002: CRITICAL CYBER ASSET IDENTIFICATION

In accordance with NERC CIP-002, the ISO will develop a list of CAs and CCAs associated with the reliable operations of the Bulk Electric System. The CA list will be developed using the risk-based methodology of a Bulk Electric System impact analysis to identify which CAs under the ISO controls support the Bulk Electric System. The CA list will be used as the basis to identify and develop a list of CCAs that are essential to the operations of the CAs.

At a minimum, both the CA and CCA lists will be reviewed using the ISO-developed risk-based assessment methodology, and approved annually by the senior manager or delegate.

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

2.1 ROLES AND RESPONSIBILITIES

2.1.1 Manager of Information Security

The manager of information security is responsible for facilitating and managing the process to identify CAs and CCAs. Additionally, this manager is responsible for annually approving both the CA and CCA lists for the purpose of CIP-002.

2.1.2 Manager from Grid and Market Operations

A manager from each of these business units is responsible for identifying the CAs required for the ISO to support the Bulk Electric System.

2.1.3 Manager of Physical Security

The manager of physical security is responsible for identifying the physical building assets required for the ISO to support and protect the CAs identified by the managers from Grid and Market Operations.

2.1.4 Information Technology Managers

All Information Technology managers are responsible for identifying the cyber assets required for the ISO to support and protect the CAs identified by the managers from Grid and Market Operations.

3 CIP-003: SECURITY MANAGEMENT CONTROLS

3.1 CYBER SECURITY POLICY


The NERC CIP Security Policy will be reviewed and approved annually by the senior manager. This policy will be available to all personnel who have access to, or are responsible for, CCAs on the intranet portal site and at physical locations outside the Physical Security Perimeter.

This policy will address the requirements in standards CIP-002 through CIP-009. Emergency situations will be addressed through the Emergency Management Program.

3.2 LEADERSHIP

The ISO will assign a senior manager to assume the overall responsibility for leading and managing the ISO's implementation and adherence to NERC CIP standards. The senior manager will have the authorization to delegate specific tasks of the program to other individual(s) within the organization as deemed necessary by the senior manager.

This assignment will be done in the form of a memorandum and include the name, title, and date of designation. Additionally, any changes will be documented within thirty calendar days of the effective date.

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

3.3 EXCEPTIONS

All exceptions to the NERC CIP Security Policy must be documented and authorized by the senior manager or delegate. All exceptions must include an explanation of the reason for the exception and any compensating measures and follow the Corporate Exception to Policy Procedure.

All technical feasibility exceptions will follow the NERC CIP Technical Feasibility Exception to Policy Procedure.

Authorized exceptions will be documented within 30 days of granting the exception.

All exceptions will be reviewed and approved annually by the senior manager or delegate.

3.4 INFORMATION PROTECTION

The ISO will implement, document and maintain a program to identify, classify, and protect information associated with CCAs. This protected information will include the following, regardless of media type,


- operational procedures,
- lists as required in Standard CIP-002,
- network topology or similar diagrams,
- floor plans of computing centers that contain CCAs,
- equipment layouts of CCAs,
- disaster recovery plans,
- incident response plans, and
- security configuration information.

Information related to CCAs will be classified as “Confidential” and afforded the protection and handling as set forth in the information protection program.

An annual assessment of adherence to the information protection program will be conducted and the results documented to help assist in improving protection of CCA information.

3.5 ACCESS CONTROL

The ISO will implement, document, and maintain a program for managing access to protected CCA information. A list of designated personnel responsible for authorizing logical or physical access to protected information will be maintained and verified on an annual basis. Personnel on the list will be identified by name, title, and the information for which they are responsible for authorizing access. Access privileges will be reviewed on an annual basis. The processes for controlling access privileges to protected information will be assessed on an annual basis and the results documented.

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

3.6 CHANGE CONTROL AND CONFIGURATION MANAGEMENT

The ISO will implement, document, and maintain a process of change control for adding, modifying, replacing, or removing CCA hardware or software, and implementing supporting configuration management activities to identify, control and document all ISO or vendor-related changes to hardware and software components of CCAs pursuant to the change control process.

4 CIP-004: PERSONNEL AND TRAINING

4.1 AWARENESS

The ISO will establish, document, implement, and maintain a security awareness program. This program will be used to reinforce sound security practices to personnel having authorized cyber or authorized unescorted physical access to CCAs. This program will include awareness communications on a quarterly basis using formal communication paths such as:

- Direct communications (e.g., emails, memos, computer based training, etc.)
- Indirect communications (e.g., posters, intranet, brochures, etc.)
- Management support and reinforcement (e.g., presentations, meetings, etc.)

4.2 TRAINING

The ISO will establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to CCAs. The program must be able to demonstrate that training was conducted at least annually (plus or minus 1 month), the date of training, and attendance records. Training will take place prior to authorization for cyber and/or unescorted access to CCAs.


Additionally, annual refresher training will be conducted for personnel with cyber and/or unescorted access to CCAs on a calendar year of July 1st through June 30th. The training program shall be reviewed annually at a minimum, and updated as needed.

The training will cover the policies, access controls, and procedures as developed for the CCAs covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

- The proper use of CCAs
- Physical and electronic access controls to CCAs
- The proper handling of CCA Information
- Cyber Security Incident Response Plans and Cyber Asset Recovery Plans

4.3 PERSONNEL RISK ASSESSMENT

The ISO will maintain a documented personnel risk assessment program, in accordance with federal, state, and local laws for personnel (including contractors and service

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

vendors) that have authorized cyber or authorized unescorted physical access to CCAs. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted access.

Each personnel risk assessment will include an identity verification and seven-year criminal check (plus or minus 6 months) with the results of the assessment documented. Documentation of each assessment (including name, date of last background check, and a summary of the results) will be maintained for a minimum of seven years. Thereafter, the ISO will update the background check every seven years after the initial background check or for cause.

4.4 ACCESS

The ISO will maintain a list of all personnel with authorized cyber and/or unescorted physical access, including their access rights to CCAs. This list will be updated within seven calendar days of any change in personnel with such access to CCAs as well as reviewed on a quarterly basis. Access to CCAs will be removed within 24 hours for termination with cause and within seven days for termination without cause.

5 CIP-005: ELECTRONIC SECURITY PERIMETER

5.1 ELECTRONIC SECURITY PERIMETER

The ISO will establish, document and ensure that all CCAs reside within an electronic security perimeter. All external access points terminating at any device within the electronic security perimeter must be identified. Any non-critical CA within a defined electronic security perimeter will be protected pursuant of the NERC CIP Security Policy and CIP-005.


Cyber Assets used in the access control and monitoring of the electronic security perimeter will be protected pursuant of the NERC CIP Security Policy and NERC CIP-004, R1.5.

5.2 ELECTRONIC ACCESS CONTROLS

The ISO will document and implement the organization processes along with the technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter. Access controls to all electronic access points to the electronic security perimeter will comply with NERC CIP-005, R2.1-2.6. The ISO does not permit dial-up access to devices within an electronic security perimeter. The ISO will physically audit the devices within each electronic security perimeter at least annually, to verify that no dial-up access is enabled.

5.3 MONITORING ELECTRONIC ACCESS

The ISO will document and implement an electronic or manual process for monitoring and logging access at access points to the electronic security perimeter 24 hours a day,

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

seven days a week. Monitoring of access controls to all electronic access points to the electronic security perimeter will comply with NERC CIP-005, R3.

5.4 CYBER VULNERABILITY ASSESSMENT

The ISO will perform annual cyber vulnerability assessments of the electronic security perimeter. The assessment report will include:

- Vulnerability identification assessment process,
- A review to verify that only authorized ports and services are enabled,
- Access point discovery,
- Controls review for default accounts, passwords, and network management community strings,
- Assessment results, the action plan to remediate or mitigate vulnerabilities identified in the assessment, the execution status of the action plan.

5.5 DOCUMENTATION REVIEW AND MAINTENANCE

The ISO will review, update, and maintain all documentation to support the compliance with the requirements of CIP-005. The ISO will ensure that all documentation required by CIP-005 reflects current configurations and processes and shall be reviewed annually.

The ISO will update documentation to reflect the modification of the network or controls within ninety calendar days of the change. All electronic access logs will be retained for at least ninety calendar days. Logs related to reportable incidents will be kept three calendar years in accordance with CIP-008, R2.

6 CIP-006: PHYSICAL SECURITY

6.1 PHYSICAL SECURITY PLAN

The ISO will document, implement, and maintain a physical security plan. This plan will be approved by the senior manager or delegate and will address requirements outlined in CIP-006, R1.1-R1.8. The physical security plan will be reviewed annually.


6.2 PROTECTION OF PHYSICAL ACCESS CONTROL SYSTEMS

Cyber assets that authorize or log access to the physical security perimeter shall be protected from unauthorized physical access. They shall also be afforded the protective measures specified in CIP-003, CIP-004 R3, CIP-005 R2 & R3, CIP-006 R4 & R5, CIP-007, CIP-008, and CIP-009.

6.3 PROTECTION OF ELECTRONIC ACCESS CONTROL SYSTEMS

Cyber assets used in the access control and/or monitoring of the electronic security perimeter shall reside within an identified physical security perimeter.

6.4 PHYSICAL ACCESS CONTROLS

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

The ISO will document, implement, and maintain operational and procedural controls to manage physical access to all access points to the physical security perimeter 24 hours a day, seven days a week. Physical access methods to physical security perimeter, such as a card-key, special lock, security personnel controlling access, or other authentication devices will be used.

6.5 MONITORING PHYSICAL ACCESS

The ISO will document and implement technical and procedural controls for monitoring physical access at all access points to the physical security perimeter 24 hours a day, seven days a week. Unauthorized access attempts will be reviewed immediately and handled in accordance with the procedures specified in CIP-008.

6.6 LOGGING PHYSICAL ACCESS

The ISO will document and implement the technical and procedural mechanisms for logging physical entry at all access points to the physical security perimeter. The logging will record sufficient information to uniquely identify the individual and the time of access 24 hours a day, seven days a week. Logging methods may include computerized logging, video recording, manual logging or their equivalent.

6.7 ACCESS LOG RETENTION

The ISO will retain physical access logs to the physical security perimeter for at least ninety calendar days. Logs related to reportable incidents will be kept three calendar years in accordance with the requirements of CIP-008.

6.8 MAINTENANCE AND TESTING


The ISO will implement maintenance and testing programs to ensure that all physical security systems under CIP-006, R4-R5, function properly. The program will include:

- Testing and maintenance of all physical security mechanisms on a cycle no longer than three years,
- Retention of testing and maintenance records for the cycle of four years, and
- Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

7 CIP-007: SYSTEMS SECURITY MANAGEMENT

7.1 TEST PROCEDURES

The ISO will perform testing to ensure that existing cyber security controls are not adversely affected by the addition of new cyber assets or significant changes to existing cyber assets within the electronic security perimeter. For the purpose of this policy, a significant change, at a minimum, includes the implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

The ISO will create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on production systems or its operations. Security testing will be performed in a manner that reflects the production environment and test results will be documented.

7.2 PORTS AND SERVICES

The ISO will ensure that only those ports and service required for normal and emergency operations are enabled on cyber assets within the electronic security perimeter. All ports and services not required for normal and emergency operations will be disabled. Where unused ports and services cannot be disabled due to technical limitations, compensating measures will be applied and documented to mitigate risk exposure.

7.3 SECURITY PATCH MANAGEMENT

The ISO will develop and maintain a program for the tracking, evaluation, testing, and installation of applicable cyber security patch for cyber assets within the electronic security perimeter. The assessment of security patches and security upgrades will take place within thirty calendar days of availability from the vendor. The results of the assessment installation will be documented. Implementation of approved patches will be documented. In any case where the patch is not installed, compensating measures will be documented and applied to mitigate risk exposure.

7.4 MALICIOUS SOFTWARE PREVENTION


The ISO will utilize anti-virus software and other malicious software prevention tools to protect CAs within the electronic security perimeter to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware. The ISO will document this implementation as well as the process used to update prevention signatures. The update process will address the testing and installation of signatures.

7.5 ACCOUNT MANAGEMENT

The ISO will establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for all user activity, and that minimize the risk of unauthorized system access. These controls will be consistent with the concept of “need-to-know” with respect to work functions. No user will be allowed access to an information resource unless authorized by designated ISO management.

Information systems will be configured or a process developed to generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

All administrator, shared, factory default accounts and other generic account privileges will be identified and placed under management control. The designated manager is responsible for the use of the shared account and must control access to the password. Where possible, these accounts will be removed or disabled. In cases where they cannot

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

be removed or disabled, the password will be changed prior to putting the system into service. Personnel with access to shared accounts will be identified and documented.

At a minimum, the ISO will require the use of passwords with the following parameters, as technically feasible;

- a minimum of six characters;
- consist of a combination of alpha, numeric, and special characters; and
- shall be changed at least annually

7.6 SECURITY STATUS MONITORING

The ISO will implement technical and/or procedural controls to monitor system events related to security, review and alert upon detection of an event on all cyber assets with the electronic security perimeter. Logs of system events related to cyber security will be retained for ninety calendar days. Additionally, security events related to CCAs will be kept for three calendar years and comply with requirements set forth in CIP-008, R2.

7.7 DISPOSAL OR REDEPLOYMENT

The ISO will establish formal methods, processes, and procedures for the disposal or redeployment of all cyber assets within the electronic security perimeter. Prior to disposal or redeployment of such assets, the ISO will erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data. The ISO will maintain records for both events.

7.8 CYBER VULNERABILITY ASSESSMENT

The ISO will perform annual cyber vulnerability assessments of all CCAs within the electronic security perimeter. The assessment report will include:


- Identification of the vulnerability assessment process;
- A review to verify that only authorized ports and services are enabled;
- Review of controls for default accounts; and
- Results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, the execution status of the action plan.

7.9 DOCUMENTATION REVIEW AND MAINTENANCE

On an annual basis, the ISO will review all documentation to support the compliance with the requirements of CIP-007. The ISO will update documentation to reflect changes resulting from modifications of the systems or controls within ninety calendar days of the change.

8 CIP-008: INCIDENT REPORTING & RESPONSE PLANNING

8.1 CYBER SECURITY INCIDENT RESPONSE PLAN

	Enterprise Policy Information Security	Effective Date	11/30/2011
	NERC CIP Security Policy		Version
Review By			11/30/2012

The ISO will develop, maintain, and implement a Cyber Security Incident Response Plan. The plan will include:

- Procedures to characterize and classify events as reportable Cyber Security Incidents,
- Response action, including roles and responsibilities of Cyber Security incident response teams, incident handling procedures, and communication plans,
- Process for reporting all events classified as cyber security incidents of CCAs to the Electricity Sector Information Sharing and Analysis Center,
- Process to update the plan within thirty calendar days of any changes,
- Process to review the plan annually, and
- Process for ensuring the response plan is tested at least annually.

A test of the response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

8.2 CYBER SECURITY INCIDENT DOCUMENTATION

The ISO will keep relevant documentation related to events classified as cyber security incidents of CCAs for three calendar years.

9 CIP-009: RECOVERY PLANS FOR CRITICAL CYBER ASSETS

9.1 RECOVERY PLANS

The ISO will create and annually review recovery plans for all CCAs and cyber assets used in the access control and monitoring of electronic security perimeters. These plans will specify the required actions in response to events or conditions of varying duration and severity. It will also include the roles and responsibilities of responders.

9.2 EXERCISES


The ISO will perform an annual exercise to test the recovery plans related to CCAs. The exercise can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

9.3 CHANGE CONTROL

The ISO will apply the enterprise information security policy regarding recovery plan change control. Additionally, changes to recovery plans associated with CCAs shall be communicated to personnel responsible for the activation and implementation of the recovery plan within thirty calendar days of the change.

9.4 BACKUP AND RESTORE

The ISO recovery plans will include processes and procedures for the backup and storage of information required to successfully restore CCAs.

 California ISO <i>Shaping a Renewed Future</i>	Enterprise Policy Information Security	Effective Date	11/30/2011
NERC CIP Security Policy		Version	1.6
		Review By	11/30/2012


9.5 TESTING BACKUP MEDIA

Information essential to the recovery of CCAs that is stored on backup media shall be tested annually to ensure that the information is available.

10 EMERGENCY PROVISIONS

During a declared health, safety (fire, law enforcement), adverse weather or system emergency involving assets covered under this Cyber Security Policy, it may become necessary to deviate from policies and procedures until an end to the emergency has been declared or such time that the provisions can be reinstated without health or safety risk. The declaration of such emergencies may be based on Standard Operating Procedures or by external entities such as health, safety or security officials.

Once the emergency situation has ended or the need for deviation from the Cyber Security Policy has ended, actions must be taken to assure restoration of security practices and to ensure security has not been compromised during the deviation period. All emergency situation documentation must be recorded as an exception to policy.

 California ISO <i>Shaping a Renewed Future</i>	Enterprise Policy Information Security	Effective Date	11/30/2011
NERC CIP Security Policy		Version	1.6
		Review By	11/30/2012

11 POLICY APPROVAL

Petar Ristanovic, VP of Technology

Print Name and Title

Signature

Date
