


CIP CYBER SECURITY POLICY

	* Category:	Critical Infrastructure Protection	
	Type:	Cyber Security	
	Document:	CIP-065	
	Owner:	Michael Pokas, Director, Information Technology Services	
	Eff. Date/Rev. #	05/23/2012	010
	Approval:	Denis DesRosiers, Vice President IT & CIO	

* References to ITC are references to ITC Holdings Corp. together with all of its subsidiaries, unless otherwise noted.

1. INTRODUCTION

- 1.1. This document replaces CIP-065 Revision 009, dated 02/22/2012 and titled "CIP Cyber Security Policy".
- 1.2. This document serves to satisfy the procedure requirements set forth in the following standards and will be reviewed annually as indicated by the "Next Annual Review" date which is 3rd Quarter 2012.
 - 1.2.1. NERC Cyber Security Standards CIP-002 through CIP-009
- 1.3. This document represents ITC's Cyber Security Policy and reflects ITC management's commitment and ability to secure ITC Critical Cyber Assets. This policy requires that ITC maintain an effective level of cyber security and provides a framework for compliance with NERC CIP standards CIP-002 through CIP-009 including provisions for emergency situations

2. SCOPE AND RESPONSIBILITY

- 2.1. ITC information security policies apply to all ITC employees, contractors, consultants, temporary employees and interns that will be collectively referred to herein as ITC resources.
- 2.2. ITC management is responsible for ensuring that all ITC policies and associated standards and guidelines are properly communicated, understood and enforced within their respective departments.
- 2.3. ITC resources are required to understand their roles and responsibilities related to the protection of organizational assets and to familiarize themselves with this and all other ITC policies, procedures and standards regarding information security.
- 2.4. The Director, Information Technology Services is responsible for ensuring that the document is made available to all ITC resources.

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CIP CYBER SECURITY POLICY

- 2.5. This policy shall be reviewed and approved annually by the CIP Senior Manager Designate, as identified in the CIP-052 CIP Senior Manager Designate document and the Director, Information Technology Services.
- 2.6. Any ITC resource found to have violated this or any ITC policy may be subject to disciplinary action, up to and including termination of employment.

3. REFERENCES

- 3.1. Due to the nature of this document references are embedded throughout the document rather than compiled here.

4. PRECAUTIONS

- 4.1. N/A

5. CIP CYBER SECURITY POLICY

5.1. Critical Cyber Asset Identification

- 5.1.1. **Policy:** A procedure will be created and maintained to identify and document a risk-based assessment methodology to facilitate the identification of critical assets and critical cyber assets.
 - 5.1.1.1. A list of Critical Assets determined through an annual application of the risk-based assessment methodology must be created.
 - 5.1.1.2. The documented list of critical assets and critical cyber assets shall be reviewed and approved annually.
 - 5.1.1.3. The CIP Senior Manager Designate shall approve annually the risk based methodology, list of Critical Assets and the list of Critical Cyber Assets.
- 5.1.2. **NERC Standard:** CIP-002 R1, R2, R3, R4
- 5.1.3. **Documentation:**
 - 5.1.3.1. CIP-041 Critical Asset Identification
 - 5.1.3.2. CIP-541 Critical Asset & Critical Cyber Asset List

5.2. NERC CIP Leadership

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CIP CYBER SECURITY POLICY

- 5.2.1. **Policy:** ITC shall identify a Senior Manager Designate responsible for the implementation, governance and ongoing compliance with the NERC Critical Infrastructure Protection (CIP) standards CIP-001 through CIP-009.
 - 5.2.1.1. The NERC CIP Senior Manager Designate will be appointed and approved by the COO of the organization.
 - 5.2.1.2. The NERC CIP Senior Manager Designate shall be identified by name, title, and date of designation.
 - 5.2.1.3. Where allowed by Standards CIP-002 through CIP-009, the Senior Manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the Senior Manager.

5.2.2. **NERC Standard:** CIP-003 R2

5.2.3. **Documentation:**

- 5.2.3.1. CIP-052 CIP Senior Manager Designation

5.3. Information Protection

- 5.3.1. **Policy:** Information associated with critical systems shall be identified, documented and protected through an established information protection program.
 - 5.3.1.1. The program shall identify and document information associated with critical systems.
 - 5.3.1.2. All information related to critical systems will be classified based on the sensitivity of the information.
 - 5.3.1.3. The effectiveness of the information protection system will be assessed annually and the results of this assessment must be retained.
 - 5.3.1.4. A mitigation plan shall be created and executed to address any deficiencies identified by the assessment.

CIP CYBER SECURITY POLICY

5.3.2. The Information Protection program may be temporarily suspended during an emergency as declared under this document name. However, the program will be reinstated as soon as feasibly possible.

5.3.3. **NERC Standard:** CIP-003 R4

5.3.4. **Documentation:**

5.3.4.1. CIP-018 Critical Cyber Asset Information Classification Process

5.3.4.2. CIP-058 Critical Cyber Asset Information Access Control

5.4. Access Control and Monitoring

5.4.1. **Policy:** To maintain the availability, integrity and confidentiality of critical systems, access to such systems will be tightly controlled and monitored.

5.4.2. Access to Critical Cyber Asset information is authorized by ITC Resources identified as Access Controllers within the CIP-019 Access Controller and Change Controller Lists document.

5.4.3. In accordance with NERC CIP Standard CIP-004 Requirement 4, ITC is required to maintain a list of personnel with authorized cyber or authorized unescorted physical access to critical cyber assets. This list must be reviewed and updated on a quarterly basis.

5.4.4. Appropriate Use Banners shall be displayed on the user screen upon all interactive access attempts on electronic access control devices where technically feasible and maintain a document identifying the content of the banner.(CIP-071 Logon Banner Standard)

5.4.5. The Access Control process has technical and procedural controls that enforce access authentication of, accountability for, all user activity, and that minimize the risk of unauthorized system access.

5.4.6. As part of the Monitoring process ITC ensures that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools, or organizational process

CIP CYBER SECURITY POLICY

controls to monitor system events that are related to cyber security.

- 5.4.7. The Access Control and monitoring processes may be suspended during emergencies. However, these processes will be reinstated as soon as feasibly possible as declared under this document name.

- 5.4.8. **NERC Standard:**

- 5.4.8.1. CIP-003 R5, CIP-004 R4, CIP-005 R2, R3, R4
CIP-006 R2, R3, R4, R5, CIP-007 R5, R6

- 5.4.9. **Documentation:**

- 5.4.9.1. CIP-019 Access Controller and Change Controller Lists
 - 5.4.9.2. CIP-043 Critical Asset and Critical Cyber Asset Access Review
 - 5.4.9.3. CIP-045 Electronic Security Perimeters
 - 5.4.9.4. CIP-047 Security Control Testing Process
 - 5.4.9.5. CIP-058 Critical Cyber Asset Information Access Control
 - 5.4.9.6. CIP-073 Account Management and Logging Policy
 - 5.4.9.7. CIP-076 Password Protection For CIP Use Only Procedures
 - 5.4.9.8. CIP-077 Integrated Security Solution
 - 5.4.9.9. SEC-003 Physical Security Policy
 - 5.4.9.10. SEC-036 Access Control

- 5.5. **Change Control and Configuration Management**

- 5.5.1. **Policy:** All hardware, software and configuration changes will be tested, approved and documented prior to being placed in the production environment.

CIP CYBER SECURITY POLICY

5.5.1.1. All such changes will be approved by the appropriate Change Controller prior to testing and again before being promoted to production.

5.5.1.2. The Change Control Process may be suspended during emergencies as declared under this document name. However, formal testing and documentation of all changes placed in production during an emergency will be performed as soon as feasibly possible.

5.5.2. **NERC Standard:** CIP-003 R6, CIP-007 R1

5.5.3. **Documentation:**

5.5.3.1. CIP-019 Access Controller and Change Controller Lists

5.5.3.2. CIP-055 Change Control & Configuration Management

5.5.3.3. CIP-047 Security Control Testing Process

5.6. Cyber Security Training and Awareness

5.6.1. **Policy:** ITC will document, implement and maintain a security awareness and cyber security training program for all personnel having authorized cyber access or authorized unescorted physical access to critical cyber assets.

5.6.1.1. The training shall cover security policies, physical and cyber access controls, critical information handling, incident response procedures and the disaster recovery procedures.

5.6.1.2. The training shall be conducted on an annual basis.

5.6.2. **NERC Standard:** CIP-004 R1, R2

5.6.3. **Documentation:**

5.6.3.1. CIP-051 Security Awareness and Cyber Security Training Policy

5.7. Personnel risk Assessment

5.7.1. **Policy:** A personnel risk assessment program is created, maintained and documented for all personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. Prior to being allowed cyber or unescorted physical access to any ITC cyber assets or facilities, a Personnel Risk Assessment (PRA) shall be conducted except in specified circumstances such as an emergency.

5.7.1.1. The program will be conducted in accordance with existing federal, state and local laws and be administered by the Human Resources department.

5.7.1.2. Each PRA assessment shall minimally include:

5.7.1.2.1. Identity verification (e.g. Social Security Number verification in the U.S.)

5.7.1.2.2. Driver's license status and history check

5.7.1.2.3. Seven year criminal check

5.7.1.2.4. Check of a terrorist watch list

5.7.1.3. Once it is received, the PRA is reviewed by the Physical Security group to determine if the required criteria are listed in the document.

5.7.1.4. Each risk assessment shall be updated at least every seven years after the initial PRA date or for cause.

5.7.1.5. The PRA reports shall be stored in the ITC Access Request System.

5.7.2. **NERC Standard:** CIP-004 R3

5.7.3. **Documentation:**

5.7.3.1. SEC-007 Employment Personnel Risk Assessment Policy.

5.8. Electronic Security Perimeter

CIP CYBER SECURITY POLICY

5.8.1. **Policy:** A clearly defined Electronic Security Perimeter (ESP) shall be established around networks containing critical cyber assets and all access points will be defined.

5.8.1.1. In accordance with the NERC CIP standard CIP-005 R1, ITC will ensure that every Critical Cyber Asset resides within a clearly identified ESP, with all access points documented.

5.8.2. **NERC Standard:** CIP-005 R1

5.8.3. **Documentation:**

5.8.3.1. CIP-045 Electronic Security Perimeters

5.9. Cyber Vulnerability assessment

5.9.1. **Policy:** A Network Vulnerability assessment process shall be developed and will include scanning, risk analysis and reporting.

5.9.1.1. The vulnerability assessment of the electronic access points to the ESP's will be performed at least annually.

5.9.1.2. A review must be performed to verify that only ports and services required for operations at these access points are enabled.

5.9.1.3. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan must be created.

5.9.2. **NERC Standard:** CIP-005 R4, CIP-007 R8

5.9.3. **Documentation:**

5.9.3.1. CIP-050 Network Vulnerability Assessment Process

5.10. Physical Security Planning, Testing and Maintenance

5.10.1. **Policy:** An ITC Physical Security Policy document has been developed and documented.

CIP CYBER SECURITY POLICY

- 5.10.1.1. The document serves to identify and describe the various components, policies and procedures that encompass the total ITC Physical Security Plan as well as the measures, processes, tools, and procedures to monitor physical access to the perimeter(s).
- 5.10.1.2. Each Physical Security Perimeter (PSP) shall consist of a “six-wall” enclosed boundary, where feasible.
- 5.10.1.3. Cyber assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.
- 5.10.1.4. Entry or attempted entry to each PSP will be monitored on a 24/7 basis, logged and unauthorized attempts will be investigated and any action taken documented.
- 5.10.1.5. Access logs will be retained for at least ninety days and logs related to reportable incidents will be kept in accordance with the requirements of standard CIP-008.
- 5.10.1.6. Authorized access will be clearly defined and shall include provisions for visitor and vendor access.
- 5.10.1.7. Individuals not authorized for unescorted access shall be escorted at all times.
- 5.10.1.8. The Physical Security Policy shall be updated within thirty days of any redesign or reconfiguration of any plan component.
- 5.10.1.9. Corporate Security shall at a minimum test all physical security mechanisms every 3 calendar years.
- 5.10.1.10. Evidence of physical security mechanism testing shall be documented on a site specific testing log which shall be prepared by the individual conducting the testing.

5.10.2. **NERC Standard:** CIP-006 R1, R3, R4, R5,R6, R7, R8

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CIP CYBER SECURITY POLICY

5.10.3. Documentation:

- 5.10.3.1. SEC-003 Physical Security Policy
- 5.10.3.2. SEC-036 Access Control
- 5.10.3.3. CIP-043 Critical Cyber Asset Access Review
- 5.10.3.4. SEC-004 Sabotage Reporting
- 5.10.3.5. SEC-062 Physical Security Review and Update Process
- 5.10.3.6. SEC-067 Physical Security Mechanisms Testing & Maintenance

5.11. Ports and Services

5.11.1. Policy: Only ports and services required for operation shall be enabled.

- 5.11.1.1. ITC shall perform a cyber Vulnerability Assessment (VA) of the electronic access points to the ESP's annually.
- 5.11.1.2. The VA shall include a review to verify that only ports and services required for operations at these access points are enabled.
- 5.11.1.3. Security Control Testing will include a process to ensure that ports and services enabled are ones required for normal or emergency operation of the system. All other ports and services should be disabled.

5.11.2. NERC Standard: CIP-005 R2, R4 CIP-007 R2, R8

5.11.3. Documentation:

- 5.11.3.1. CIP-050 Network Vulnerability Assessment Process
- 5.11.3.2. CIP-047 Security Control Testing Process

5.12. Security Patch Management

- 5.12.1. **Policy:** An ITC security patch management program shall be established, documented and implemented for tracking, evaluating, testing and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter (s).
- 5.12.1.1. An ITC resource assigned by a Change Controller will perform a manual Internet search on a weekly basis to determine availability of anti-virus and malware prevention signature updates.
- 5.12.1.2. When a newly available signature is identified, it is downloaded to the appropriate test system.
- 5.12.1.3. Within thirty days of the date a security patch becomes available, it shall be evaluated for applicability to installed devices or applications.
- 5.12.1.4. Any patch deemed applicable shall be tested and an implementation plan developed.
- 5.12.1.5. The system receiving the updated signature will be observed for a period of time adequate to determine that the production system is operating correctly.
- 5.12.1.6. Upon successful installation of a signature appropriate changes or updates will be made to the Anti-Virus Signature Configuration Document.
- 5.12.2. **NERC Standard:** CIP-007 R3
- 5.12.3. **Documentation:**
- 5.12.3.1. CIP-061 Security Patch Management Process
- 5.12.3.2. CIP-019 Access Controller and Change Controller Lists

5.13. Malicious software Prevention

- 5.13.1. **Policy:** Systems within an ESP shall implement Anti-virus and malicious software prevention measures. Where technically feasible, these measures shall include host-based anti-virus software.

CIP CYBER SECURITY POLICY

5.13.2. **NERC Standard:** CIP-007 R4

5.13.3. **Documentation:**

5.13.3.1. CIP-006 Anti-virus Standards

5.13.3.2. CIP-066 Anti-virus Signature Update Process

5.14. System Disposal or Redeployment

5.14.1. **Policy:** ITC will employ formal methods processes, and procedures for disposal or redeployment of Critical Cyber Assets within the ESP.

5.14.1.1. This process applies only to the retirement of ITC IT assets, including but not limited to desktop computers, laptops, servers, monitors, keyboards, storage media, copy machines, fax machines and printers.

5.14.1.2. ITC personnel must follow a set of defined measures to properly destroy data on servers, desktop computers, and other IT assets scheduled for retirement.

5.14.2. **NERC Standard:** CIP-007 R7

5.14.3. **Documentation:**

5.14.3.1. CIP-053 IT Asset Retirement and Redeployment Process

5.15. Incident Response

5.15.1. **Policy:** A cyber security incident response plan shall be developed and will include:

5.15.2. Documented steps necessary for effectively and efficiently managing a cyber security incident.

5.15.2.1. Include procedures to characterize and classify events as reportable Cyber Security Incidents.

5.15.2.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

CIP CYBER SECURITY POLICY

5.15.2.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC).

5.15.2.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

5.15.2.5. Process for ensuring that the Cyber Security Incident response plan is reviewed and tested at least annually.

5.15.3. **NERC Standard:** CIP-008 R1, R2

5.15.4. **Documentation:**

5.15.4.1. CIP-068 Cyber Security Incident Response Plan

5.16. **Business Continuity and Disaster Planning**

5.16.1. **Policy:** A disaster recovery and business continuity plan will be created and implemented.

5.16.1.1. Create and annually review recovery plan(s) for Critical Cyber Assets.

5.16.1.2. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

5.16.1.3. Define the roles and responsibilities of responders.

5.16.1.4. The recovery plan(s) shall be exercised at least annually.

5.16.1.5. Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.

5.16.1.6. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change.

5.16.1.7. The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical

CIP CYBER SECURITY POLICY

Cyber Assets. Backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

- 5.16.1.8. Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available.

5.16.2. **NERC Standard:** CIP-009 R1, R2, R3, R4, R5

5.16.3. **Documentation:**

- 5.16.3.1. CIP-084 Critical Asset Recovery Plan.

5.17. Emergency Situations.

- 5.17.1. Electric utility emergency situations include emergencies that threaten the operational reliability of the bulk electric system, situations when restoration of a critical service is required, or an emergency affecting a Critical Cyber Asset.
- 5.17.2. An emergency situation could also include any other unexpected occurrences. This could include storms floods, fires, malicious acts or other similar special operating situations.
- 5.17.3. During an emergency situation certain ITC policies and/or procedures could be temporarily suspended. However, any such suspensions will be reinstated immediately after the emergency has passed. Considerations for temporary suspension include:
 - 5.17.3.1. Emergency changes to Critical Cyber Assets required during emergency situations within its change management procedures (CIP-055 Change Control & Configuration Management).
 - 5.17.3.2. The Information Protection program (CIP-018 Critical Cyber Asset Information Classification Process).
 - 5.17.3.3. The access control process (CIP-058 Critical Cyber Asset Information Access Control) may be suspended during emergencies. However, the

CIP CYBER SECURITY POLICY

process will be reinstated immediately after the emergency is over.

5.17.3.4. Other Cyber security policies as required.

5.18. Exceptions

- 5.18.1. In an instance where ITC or an ITC resource cannot conform to one or more information security policies or associated standards, the circumstances must be documented as an exception and authorized by the ITC Senior Manager designate.
- 5.18.2. In accordance with NERC standard CIP-003 Requirement 3, exceptions to any information security policy or standard must be authorized by the ITC Senior Manager designate as identified in the CIP-052 Senior Manager Designate document.
- 5.18.3. Requests for exceptions to any ITC security policy must be submitted in writing using the CIP-065 F1 Cyber Security Policy Exception Request Form to the Director, Information Technology Services.
- 5.18.4. The request will be evaluated by the Director, Information Technology Services, then approved or rejected. Once approved, it will also be signed by the Senior Management Designate.
- 5.18.4. Approved exceptions shall be documented in the Cyber Security Policy Exceptions List (CIP-065-L1).
 - 5.18.4.1. Documentation must include an explanation of the exception, why the exception is necessary and applicable compensating measures associated with granting the exception.
 - 5.18.4.2. Explanation should include the specific standard and/or policy the exception is for.
 - 5.18.4.3. Documentation shall be completed within thirty days of the approval.
 - 5.18.4.4. The Cyber Security Policy Exceptions List will be signed by the Senior Manager Designate.

CIP CYBER SECURITY POLICY

- 5.18.5. Authorized exceptions shall be reviewed, documented and approved by the Senior Manager Designate annually to ensure the exceptions are still required and valid.

5.19. Documentation Review and Maintenance for NERC CIP-005 and CIP-007

- 5.18.6. ITC will review update and maintain all documentation to support compliance with the requirements of NERC CIP-005 and CIP-007 as stated in the CIP-070 CIP Security Management Documentation Review document.
- 5.18.7. CIP-005 and CIP-007 documentation will be reviewed at least annually by the subject matter experts and/or document owners and the CIP Steering Committee.
- 5.18.8. CIP Documents shall be updated to reflect modifications to the network or controls within thirty calendar days of the change in accordance with NERC CIP-005 Requirement 5.
- 5.18.9. CIP Documents shall be updated to reflect modifications to the systems or controls within thirty calendar days of the change in accordance with NERC CIP-007 requirement 9.

6. ATTACHMENTS

- 6.1. CIP-065 Att99 Annual Review Internal-Attachment 99
- 6.2. CIP-065-L1 Cyber Security Policy Exceptions

7. MISCELLANEOUS

- 7.1. N/A

CIP CYBER SECURITY POLICY

8. APPROVALS

Owner: _____ <Signature on file> Date: 05/16/2012

Approver: _____ <Signature on file> Date: 05/16/2012

9. REVISION HISTORY

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
06/25/08	000	M. Pokas	Created to outline the overall cyber security policy in accordance with NERC CIP Standards 002 – 009.
10/29/08	001	L. Trammer	Transferred document ownership to M. Pokas.
06/24/09	002	M. Ensink	Changed SSE to CIP
10/30/09	003	M. Ensink	Added section 5.17 Emergency Situations Corrected CIP-018 title
11/24/09	004	M. Ensink	Added missing references to current documents in section 5.4 – CIP-073 Account Management and Logging Policy, 5.7 – corrected title should be SEC-007 Employment Personnel Risk Assessment Policy, 5.8 – added NERC Standard CIP-007 R6 and CIP-077 Integrated Security Solution, and 5.10 – added Standard CIP-006 R6
03/31/10	005	M. Ensink	Changed Section 1.2 Attachment 99 verbiage from periodically too annually. Changed the following sections for CIP standards version 2 changes 90 to 30 days. Sections 5.10.1.6 – physical security policy, 5.15.2.4 – incident response plan and 5.16.1.6 recovery plan updates need to be completed within 30 days of the change. Added section 5.2.1.3 to match new CIP-003 R2.3 verbiage allowing the senior manager to delegate specific actions where allowed in CIP standards CIP-002 through CIP-009.

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CIP CYBER SECURITY POLICY

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
06/30/10	006	M. Ensink	<p>Added sections 5.4.2 and 5.4.3 to better define the access controller who approves access to CCAs and are identified in CIP-019</p> <p>Added CIP-019 as reference document to sections 5.4.6.1, 5.5.3.1, and 5.12.3</p> <p>Added section 5.4.4 for appropriate Use Banners</p> <p>Updated section 5.6.1 to match standard verbiage to document, implement and maintain a security awareness program, and changed systems to cyber assets.</p> <p>Updated section 5.7.1 to match standard verbiage for authorized cyber and authorized unescorted physical access and verbiage for emergency situations.</p> <p>Changed 30 to thirty in section 5.10.1.6</p> <p>Changed minimally to at a minimum in section 5.10.1.7</p> <p>Added Section 5.18 for Exception process (from CIP-060)</p> <p>Added Section 4.19 for Documentation Review Process for CIP-005 R5 and CIP-007 R9 (from CIP-070)</p>

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CIP CYBER SECURITY POLICY

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
08/25/10	007	M. Ensink	<p>Section 5.4.5 - Added specific reference to CIP-007 R5 for technical and procedural controls to minimize unauthorized access.</p> <p>Section 5.4.6. - Added specific reference to CIP-007 R6 ensuring cyber assets within the ESP as technically feasible will be monitored.</p> <p>Section 5.4.8.1 - Removed CIP-007 R1 and added CIP-007 R6.</p> <p>Section 5.8.2. - Removed references to CIP-007 R6.</p> <p>Section – 5.8.3 - Removed reference to document CIP-077.</p> <p>Section 5.10.1.3. - Added specific reference to CIP-008 R3 that an ESP will reside in a PSP.</p> <p>Section 5.10.1.4 - Added “monitored on 24/7 basis”.</p> <p>Section 5.10.1.5 - Added specific reference to CIP-008 R7 (was R5) for log retention and complies with standard CIP-008.</p> <p>Section 5.10.2 - Added CIP-006 requirements R3, R4, R5, R7, and R8 that were being addressed but not listed.</p> <p>Added CIP-009 R5 to section 5.16.2, requirement is addressed in section 5.16.1.8 but not listed.</p>
03/30/11	008	C. Lewis	<p>Changed Mike Pokas' title throughout to Director, Information Technology Services</p> <p>Deleted:</p> <p>Section 5.15.4.2. - CIP-568 Cyber Security Incident Response Responsibilities Matrix</p> <p>Section 5.15.4.3. - CIP-069 Security Incident Response Testing Process</p> <p>Section 5.15.4.4. - CIP-083 Security Incident Response Review Process ...content from these documents has been incorporated into CIP-068.</p>

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CIP CYBER SECURITY POLICY

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
02/22/12	009	A. Cook G. Elliott	Updated Introduction 1.2 to state "This document serves to satisfy the procedure requirements set forth in the following standards and will be reviewed annually as indicated by the "Next Annual Review" date which is 3rd Quarter 2012." Converted "Cyber Security Policy Exceptions" document into CIP-065-L1 Inserted reference to CIP-065-L1 into Sections 5.18.5 and 6 Sections 5.7.1 and 5.7.1.2 – strengthened the wording regarding the fact that a PRA must be done before unescorted access may be given. Section 5.7.1.2 – separately listed the minimum items required on a PRA Section 5.7.1.3 – added stating the PRAs are reviewed for acceptance by the Physical Security group.
05/23/12	010	G. Elliott	Header: removed Elizabeth Howell and Steve Stout as Approvers. Section 5.18.4 - removed the original of this section that talked about what should be included in the Exception form. Section 5.18.4 – added if Exception request is approved, it must also be signed by the Senior Management Designate. Section 5.18.5.1 – added "why the exception is necessary".

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed