INFORMATION SECURITY POLICIES

*	Category:	Critical Infrastructure Protection	
	Type:	Cyber Security	
	Document:	CIP-060	
	Owner:	Mike Pokas, Director, Information Technology Services	
	Eff. Date/Rev.	03/30/2011	008
	Approval:	Denis DesRosiers, Vice President, IT & CIO Steve Stout, Director, Asset Management Elizabeth Howell, Vice President, Operations	

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

1. INTRODUCTION

1.1. This procedure replaces CIP-060 Revision 007, dated 07/16/2010, and titled "Information Security Policies".

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 associated Attachment 99.

1.2.1. NERC Cyber Security Standard CIP-003 Requirement 1

1.2.2. NERC Cyber Security Standard CIP-003 Requirement 3

1.3. The purpose of this document is to define the ITC Information Security policies implemented by ITC in order to protect the confidentiality and integrity of information stored and processed on ITC systems.

1.4. The objectives of ITC's information security policies are to prevent unauthorized disclosure of or access to information stored or processed on ITC systems and to ensure that the information is available to authorized persons when required.

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 Servicesis responsible for ensuring that the document is distributed throughout the organization.

2.5. In accordance with NERC standard CIP-003 Requirement 3, exceptions to any information security policy or standard must be authorized by the CIP Senior Manager designate as identified in the CIP-052 Senior Manager designation document.

2.5.1. 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.

2.5.2. Requests for exceptions to ITC security policies and policy standards must be submitted to the CIP Senior Manager designate.

2.5.3. Approved exceptions must be documented in the Cyber Security Policy Exceptions List. Documentation will be completed within thirty days of the approval.

2.5.4. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

3. REFERENCES

3.1. NERC Cyber Security Standard CIP-003 Requirement 1

3.2. NERC Cyber Security Standard CIP-003 Requirement 3

3.3. Cyber Security Policy Exceptions List

3.4. CIP-006 Anti-Virus Standards

3.5. CIP-008 Clear Screen Standards

3.6. CIP-016 Electronic Mail Standards

3.7. CIP-018 Critical Cyber Asset Information Classification Process

3.8. CIP-019 Access Controller and Change Controller Lists

3.9. CIP-022 Mobile Computing Standards

3.10. CIP-024 Password Standards

3.11. CIP-028 Wireless Standards

3.12. CIP-043 Critical Cyber Asset Access Control

3.13. CIP-044 Acceptible Use Standards

3.14. CIP-052 CIP Senior Manager Designate

3.15. CIP-055 Change & Configuration Management Documentation Review

3.16. CIP-056 Information Security Policy Review Process

3.17. CIP-058 Critical Cyber Asset Information Access Control

3.18. CIP-059 VPN Standards

3.19. CIP-063 Server and Router Standards

3.20. CIP-065 CIP Cyber Security Policy

3.21. CIP-068 Cyber Security Incident Response Plan

4. PRECAUTIONS

4.1. N/A

5. IT SECURITY POLICIES

5.1. Acceptable Use Policy

5.1.1. ITC equipment and resources are to be used primarily for business activities and at no time are ITC resources authorized to engage in any activity that is illegal under local, state, federal or international law. Circumventing user authentication or network security for any reason is strictly prohibited.

5.2. Anti-Virus Policy

5.2.1. ITC computers must have anti-virus protection software installed and operational. The anti-virus software must be updated on a consistent basis.

5.3. Clear Screen Policy

5.3.1. To protect confidential data from unauthorized disclosure, ITC resources will lock desktop and laptop screens when leaving their work stations unattended. ITC desktops and laptops will be required to have an approved screen saver with a lock that engages after the key/board and/or the mouse have been idle for a period of 10 minutes.

5.4. Data Backup and Recovery Policy

5.4.1. Critical ITC information systems and electronic information necessary for sustaining core business operations must be copied onto secure storage media on a regular basis.

5.5. Email Use Policy

5.5.1. ITC electronic communications systems should be used for business activities only. Email messages must not contain profanity, obscenities, derogatory remarks, messages constituting sexual, ethnic, or racial harassment or unsolicited bulk mail.

5.6. Incident Handling

5.6.1. ITC resources are responsible for reporting any suspected security breaches or violations. ITC resources who suspect a security breach or violation has taken place shall follow the CIP-068 Cyber Security Incident Response Plan.

5.7. Internet Use Policy

5.7.1. ITC resources may be granted access to the Internet and other public networks for business related activities in the normal course of performing their duties. Incidental, but non-excessive personal use of company resources and Internet connectivity is permitted.

5.8. Mobile Computing Policy

5.8.1. Mobile computing and storage devices containing or accessing the information resources at ITC must be approved prior to connecting to the ITC network and must adhere to the standards issued by the Information Technology Department.

5.9. Password Policy

5.9.1. ITC resources are required to employ strong passwords as defined by the standards issued by the ITC Information Technology Department when accessing the ITC network, systems or applications.

5.10. Wireless Policy

5.10.1. Wireless access points and devices connected to the ITC network must be registered, approved and checked for proper configuration by a designated IT Services representative prior to being placed into service.

5.11. Server and Router Security

5.11.1. All ITC corporate servers, routers and switches must meet the standard configuration and protocols set forth by ITC Information Technology management. ITC corporate servers must have the most recent security patches installed on the system as soon as practical.

5.12. Security Awareness Policy

5.12.1. ITC personnel must receive ongoing training and reinforcement with regard to sound security practices.

5.13. VPN Policy

5.13.1. ITC resources utilizing Virtual Private Networks (VPN) to access the internal ITC network must have the latest anti-virus protection software package along with the latest updates and follow the necessary protocols listed in the ITC Information Technology Standards and Guidelines.

5.13.2. A VPN must be used when establishing network access connections between the ITC network and any third party networks. Prior approval by the Director, Information Technology Services must be attained and recorded before any third party network connections may be established. These VPN connections must have logging turned on, be closely monitored and alarmed, and be protected by strong firewall rules.

6. ATTACHMENTS

6.1. CIP-060-Att99 Annual Review Internal-Attachment 99

7. MISCELLANEOUS

7.1. N/A

8. APPROVALS

Owner: <Signature on file> Date: 03/25/2011

Approver: <Signature on file> Date: 03/25/2011

Approver: <Signature on file> Date: 03/25/2011

Approver: <Signature on file> Date: 03/25/2011

9. REVISION HISTORY

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
10/02/2007	000	D. DesRosiers	Initial documentation
06/12/2008	001	M. Pokas	Revised policy ownership from Denis DesRosiers
06/24/2009	002	M. Ensink	Changed SSE to CIP. Added 1.2, references and Attachment 99.
06/30/2009	003	M. Ensink	Changed 2.5.2 per committee review.
11/24/2009	004	M. Ensink	Section 2.5.3 - Added 30 day requirement that was being followed but not documented.
03/31/2010	005	A. Stefan	Section 1.2: Replaced “periodically” with the word “annually”. Section 6: Updated name of title in Section 6.1 referencing Att99.

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
06/30/2010	006	M. Ensink	Section 2.5.3 - Updated to clearly state documentation will be completed within 30 days of approval. Section 2.5.4 - Reworded to remove acceptance of risk and more closely match standard verbiage for compensating measures.
07/16/10	007	M. Ensink	Section 3 - Added document CIP-068. Section 5.1.1 - Reworded to be more realistic, use ITC equipment – primarily for business activities, removed only. Section 5.4.1 - Removed word ‘critical’ from critical electronic. Section 5.6.1 - Replaced employees with ITC resources and follow the CIP-068 Cyber Security Incident Respone Plan.

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
03/30/11	008	C. Lewis	Changed Mike Pokas' title throughout to Director, Information Technology Services. Added: Section 3.4. - CIP-006 Anti-Virus Standards Section 3.5. - CIP-008 Clear Screen Standards Section 3.6. - CIP-016 Electronic Mail Standards Section 3.7. - CIP-018 Critical Cyber Asset Information Classification Process Section 3.8. - CIP-019 Access Controller and Change Controller Lists Section 3.9. - CIP-022 Mobile Computing Standards Section 3.10. - CIP-024 Password Standards Section 3.11. - CIP-028 Wireless Standards Section 3.12. - CIP-043 Critical Cyber Asset Access Control Section 3.13. - CIP-044 Acceptible Use Standards Section 3.14. - CIP-052 CIP Senior Manager Designate Section 3.15. - CIP-055 Change & Configuration Management Documentation Review Section 3.16. - CIP-056 Information Security Policy Review Process Section 3.17. - CIP-058 Critical Cyber Asset Information Access Control Section 3.18. - CIP-059 VPN Standards Section 3.19. - CIP-063 Server and Router Standards Section 3.20. - CIP-065 CIP Cyber Security Policy Section 3.21. - CIP-068 Cyber Security Incident Response Plan Section 5.13.2. - A VPN must be used when establishing network access connections between the ITC network and any third party networks. Prior approval by the Director, Information Technology Services must be attained and recorded before any third party network connections may be established. These VPN connections must have logging turned on, be closely monitored and alarmed, and be protected by strong firewall rules.

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
03/30/11	008	C. Lewis (cont)	<u>Deleted</u> Section 5.10. - Remote Access Policy Section 5.10.1. - ITC Resources with remote access privileges to the ITC corporate network are required to ensure that their remote access connection is given the same consideration and is subject to the same controls as the user's on-site connection to the network.retiring the use of the Remote Access Standard CIP-080 Incorporating the content from the Remote Access Standard into the CIP—059 VPN Standard. Section 5.12. -Third Party Access Section 5.12.1. - ITC resources must employ an approved, secure, formalized method of internet connection between the ITC network and all third party networks. A formalized method for the request, approval and tracking of such connections must be submitted to the Director, Information Technology Services.