


CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

	*	Category:	Critical Infrastructure Protection	
	Type:	Cyber Security		
	Document:	CIP-018		
	Owner:	Mike Pokas, Director, Information Technology Services		
	Eff. Date/Rev.	05/25/2011	007	
	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 document replaces CIP-018 Revision 006, dated 03/30/2011 and titled “Critical Cyber Asset Information Classification Process.”
- 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 as described in GAP-001 Standard for Developing and Revising O&M Procedures:
 - 1.2.1. NERC Cyber Security Standard CIP-003 Requirement 4 and its sub-requirements.
- 1.3. The purpose of this document is to describe how ITC protects the confidentiality, integrity, and availability related to ITC’s Critical Cyber Assets and information pertaining to them.
- 1.4. This policy will concentrate on the identification ,classification, protection, and handling of information associated with critical cyber assets in electronic format, as well as additional controls regarding the secure handling of hard copy information.

2. SCOPE AND RESPONSIBILITY

- 2.1. This process applies to all ITC employees, contractors, consultants, temporary employees and interns that will be collectively referred to herein as ITC resources.
- 2.2. The Critical Cyber Asset Information Classification Process applies to critical cyber assets, assets that contain information about critical cyber assets and cyber assets used in access control and monitoring of the Electronic Security Perimeter (ESP) and the Physical Security Perimeter (PSP).

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

CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

2.3. Access Controllers refers to ITC resources responsible for authorizing cyber access and unescorted physical access to critical cyber assets and critical cyber asset related information within their respective areas of responsibility.

2.3.1. The current list of access controllers can be found within the Access Controller and Change Controller Lists.

2.4. The Director, Information Technology Services is responsible for facilitating the review and update of security policies, associated standards and authorized policy exceptions.

3. REFERENCES

3.1. NERC Cyber Security Standard CIP-003 Security Management Controls

3.2. CIP-058 Critical Cyber Asset Information Access Control Process

3.3. SEC-007 Employment Personnel Risk Assessment Policy

3.4. CIP-053 IT Asset Retirement Process

3.5. CIP-043 Critical Cyber Asset Access Review

3.6. CIP-019 Access Controller and Change Controller Lists

3.7. CIP-076 Password Protection For CIP Use Only Procedures

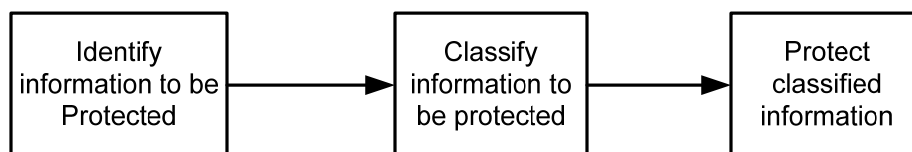
3.8. GAP-001 Standards for Developing Revising O&M Procedures.

3.9. CIP-076-L1 CIP Use Only Approved List.

4. PRECAUTIONS

4.1. N/A

5. PROCEDURE



5.1. Identify Information to be Protected

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

CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

- 5.1.1. The Access Controllers must annually identify critical cyber asset related information by filling out the Information Classification forms that applies to their area of responsibility.
- 5.1.2. It is the responsibility of the CIP Compliance Analyst to ensure that all Classification forms are reviewed, filled out, and submitted at least on an annual basis.
- 5.1.3. The following information related to critical cyber assets shall be identified, classified and protected, regardless of media type:
 - 5.1.3.1. Operational procedures.
 - 5.1.3.2. Lists of critical assets, critical cyber assets and cyber assets used in the monitoring and logging of activity at the ESP and the PSP.
 - 5.1.3.3. Network topology and similar diagrams.
 - 5.1.3.3.1. IP Address, MAC addresses, and host names
 - 5.1.3.4. Floor plans of computing centers containing critical cyber assets.
 - 5.1.3.5. Equipment layouts of critical cyber assets.
 - 5.1.3.6. Disaster Recovery plans for critical cyber assets.
 - 5.1.3.7. Incident response plans for critical cyber assets.
 - 5.1.3.8. Security Configuration information for critical cyber assets.
- 5.1.4. The items listed in section 5.1.3 shall not be electronically or in hardcopy transmitted over public networks or via external service providers unless:
 - 5.1.4.1. The hardcopy information must be sent using a carrier service approved by the CIP Compliance Manager or the Director, IT Services.

5.2. Classify Information

- 5.2.1. Information related to critical cyber assets that requires protection needs to be protected and will be classified as either CIP

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

CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

CONFIDENTIAL or INTERNAL USE ONLY in the Information Classification form.

- 5.2.2. Information classified as CIP CONFIDENTIAL refers to information whose unauthorized disclosure could seriously and adversely impact ITC and the reliable operation of the bulk electric system.
 - 5.2.2.1. CIP CONFIDENTIAL information is extremely sensitive and intended for a very limited audience within ITC.
 - 5.2.2.2. Access to CIP CONFIDENTIAL information will be tightly restricted.
- 5.2.3. Information classified as INTERNAL USE ONLY is intended for distribution and use by internal ITC resources only.
- 5.2.4. Once a document has been classified based on the sensitivity of the critical cyber asset information, one or more of the following methods may be applied to indicate its classification.
 - 5.2.4.1. Where the document is formatted as, or intended to be printed, it must contain a header or footer with the appropriate classification.
 - 5.2.4.2. Where the document is of electronic or image form intended for display on electronic media such as a computer monitor, e-reader, or portable device, an image equivalent of the appropriate classification footer must be displayed at the beginning of the document or section containing classified information.
 - 5.2.4.3. Storage of classified information that is contained within a database system or source file must be maintained in an ITC approved access controlled repository.
- 5.3. In order to access CIP CONFIDENTIAL information, resources must possess appropriate access rights and will have undergone a personnel risk assessment pursuant to SEC-007 Employment Personnel Risk Assessment Policy.
- 5.4. **Protect Sensitive Information**
 - 5.4.1. CIP CONFIDENTIAL information will be protected regardless of media type by adhering to the process outlined as well as by adhering to various other measures as outlined below.

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

CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

- 5.4.2. The documents that have been classified as CIP CONFIDENTIAL information will either have a password to protect them from being altered (CIP-076 Password Protection For CIP Use Only Procedures) or will reside in an access controlled repository.
- 5.4.3. If the recipient of any ITC information believes that the data classification is incorrect, the recipient must protect the information in a manner consistent with the more stringent of the two classifications.
- 5.4.4. If any ITC information is found to contain varying sensitivity classifications, the controls utilized must reflect the most stringent classification.
- 5.4.5. If a copier, printer or fax machine jams or malfunctions when ITC resources are processing CIP CONFIDENTIAL or sensitive information, they must not leave the machine until all copies of the information are removed from the machine or destroyed.
- 5.4.6. Computer storage media that has been used to record CIP CONFIDENTIAL information must not leave ITC control until it has been deleted or overwritten according to the published process in CIP-053 IT Asset Retirement process.
- 5.4.7. Hard copy CIP CONFIDENTIAL information must not be left unattended at any time and must be secured when not in use.
- 5.4.8. CIP CONFIDENTIAL information in hardcopy form must be disposed of in containers marked for shredding.
- 5.4.9. CIP CONFIDENTIAL and INTERNAL USE ONLY information must not be disclosed to external resources unless approval is granted by an appropriate Access Controller.

6. ATTACHMENTS

- 6.1. Information Classification Forms
 - 6.1.1. TMS Information Classification Form
 - 6.1.2. Physical Security Information Classification Form
 - 6.1.3. Field Device Information Classification Form
 - 6.1.4. CIP Information Classification Form

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

CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

6.1.5. Integrated Security Solution (ISS) Information Classification Form

6.2 CIP-018-Att99 Annual Review Internal-Attachment 99

7. MISCELLANEOUS

7.1. Compliance Verification

7.2. The following are the audit methods used:

7.2.1. Information classified as either “CIP CONFIDENTIAL” or “INTERNAL USE ONLY” will be randomly spot checked annually by the CIP Compliance Analyst.

7.2.2. After all the checks have been done the CIP Compliance Analyst will document their findings including any corrective actions that were needed.

7.2.3. The CIP Compliance Analyst will report spot checks that required corrective actions to the CIP Steering Committee. The CIP Steering Committee meeting minutes will be the proof of this action.

CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

8. APPROVALS

Owner: _____ <Signature on file> Date: 05/25/2011

Approver: _____ <Signature on file> Date: 05/25/2011

Approver: _____ <Signature on file> Date: 05/25/2011

Approver: _____ <Signature on file> Date: 05/25/2011

9. REVISION HISTORY

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
04/30/08	000	M. Pokas	Document created to satisfy NERC Standard CIP-003 Requirement 4.
10/29/08	001	L. Trammer	Transferred document ownership to M. Pokas. Added section 5.2.4 to ensure that classifications are marked appropriately.
06/24/09	002	J. Kokotovich	Added sections 5.4.1, 5.4.2, and 5.4.9. Added section 7 Changed "SSE" to "CIP" Add section 1.2 references and Attachment 99.
10/28/09	003	M. Ensink	Changed SEC-007 title to Employment Personnel Risk Assessment Policy.
03/31/10	004	A. Stefan	Section 1.2: Replaced "periodically" with the word "annually". Section 5: Added section 5.1.2 to include the CIP Compliance Managers responsibility. Section 5.1: Moved section 5.1.2 down to section 5.1.3. Section 6: Added section 6.2 referencing Att99.

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

CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
06/30/10	005	P. Melendez/T. Gruber/ A. Stefan/ M. Ensink	<p>Section 1.2.1 Added words “and its sub-requirements.</p> <p>Section 2.3.1 added the words “and Change Controller”.</p> <p>Section 3 – Added full name of CIP-003 standard and name of the CIP-019 procedure for Access and Change Controllers lists.</p> <p>Section 5.1.2 added the word “reviewed” to the role of CIP Manager to address changes for Classification forms.</p> <p>Expanded section 5.2.4 to cover more forms of information and varied application of classification indications.</p> <p>Section 5.4.2 Added “controlled repository” for documents that need altering for business processes with out password.</p> <p>Section 5.4.2 added words to allow storage of CIP confidential information.</p> <p>Section 5.4.9 Added access control as a participant of disclosing to external resources classified information.</p> <p>Replaced IT Control Manager with CIP Compliance Analyst.</p> <p>Section 7.2.4 added assess, mitigate and document to this section to cover all aspects.</p>
03/30/11	006	C. Lewis	<p>Changed Mike Pokas’ title throughout to Director, Information Technology Services</p> <p>Added CIP-076 Password Protection For CIP Use Only Procedures to the References and to section 5.4.2</p> <p><u>Changed Section 5.4.2</u> Changed From: CIP CONFIDENTIAL information must not be left unattended during non-working hours unless stored in an approved and secured enclosure To. 5.4.2. The documents that have been classified as CIP CONFIDENTIAL information will either have a password to protect them from being altered (CIP-076 Password Protection For CIP Use Only Procedures) or will reside in an access controlled repository.</p>

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

CRITICAL CYBER ASSET INFORMATION CLASSIFICATION PROCESS

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
03/30/11	006 (cont)	C.Lewis	<p>Changed Section 5.4.7 From: CIP CONFIDENTIAL information must not be left unattended during non-working hours unless stored in an approved and secured enclosure. To... Hard copy CIP CONFIDENTIAL information must not be left unattended at any time and must be secured when not in use.</p> <p>Changed Section 7.2.2 From. After all the checks have been done the CIP Compliance Analyst will document their findings including any corrective actions that were needed.</p> <p>Changed 7.2.3. From If there is an infraction found, the CIP Steering Committee will be informed immediately and will determine a timeframe for remediation. To...The CIP Compliance Analyst will report spot checks that required corrective actions to the CIP Steering Committee, and the CIP Steering Committee meeting minutes will be the proof of this action.</p> <p>Deleted: 7.2.4.The offending department will mitigate, correct and document the infraction and report back to the CIP Steering Committee.</p> <p>7.2.5. After the five business days have passed the CIP Compliance Analyst will re-audit the department.</p>
05/25/11	007	C.Lewis	<p>Added words to section 1.3 "...describe how ITC.." and to the end of the paragraph "...and information pertaining to them."</p> <p>Sections 1.2 & 3 - Added GAP-001.</p> <p>Added Section 5.1.3.3.1 IP Address, MAC addresses, and host names</p> <p>Added Section 5.1.4 and 5.1.4.1</p> <p>Changed Section 5.4.6 ..."degaussed" to "deleted"</p>

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