PASSWORD STANDARDS

*	Category:	Critical Infrastructure Protection	
	Type:	Cyber Security	
	Document:	CIP-024	
	Owner:	Mike Pokas, Director, Information Technology Services	
	Eff. Date/Rev	03/28/2012	008
	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-024 Revision 007, dated 03/30/2011 and titled “Password Standards”.

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-007 Requirement R5.3 and its sub-requirements.

1.3. The purpose of the password standards is to establish the requirements for the use of strong passwords, the protection of those passwords, and the frequency of change.

2. SCOPE AND RESPONSIBILITY

2.1. ITC management is responsible for ensuring that all ITC policies are properly communicated, understood and enforced within their respective departments.

2.2. This policy applies to all ITC employees, contractors, consultants, temporary employees and interns (referred to herein as ITC resources).

2.3. ITC resources are responsible for complying with all ITC policies and understanding their roles and responsibilities related to the protection of organizational assets.

2.4. IT Services is responsible for developing procedures for implementing this policy.

2.5. The Director, Information Technology Services is responsible for ensuring that this policy is distributed throughout the organization.

2.6. Any ITC resource found to have violated any ITC security policy may be subject to disciplinary action, up to and including termination of employment.

3. REFERENCES

3.1. NERC Cyber Security Standard CIP-007 - Security Management Controls.

4. PRECAUTIONS

4.1. N/A

5. PROCEDURE (C3R1.1)

5.1. GUIDELINES (C7R5.3)

5.1.1. All factory preset, default or standard user ID's and passwords should be removed or changed prior to deploying the resource for use in production. (C7R5.2.1)

5.1.2. ITC resources should not write down, record or store a readable password near the computing device to which it pertains.

5.1.3. ITC resources should not share their passwords with anyone, including administrative assistants, secretaries or superiors.

5.1.4. ITC resources should avoid constructing new passwords that are identical or substantially similar to passwords previously employed.

5.1.5. ITC should employ systems that prevent re-use of at least the four previous passwords employed by a user.

5.1.6. Passwords should not be inserted into electronic mail messages or other forms of electronic communication.

5.2. STANDARDS

5.2.1. ITC resources are required to use passwords when accessing the ITC corporate network systems.

5.2.2. Each ITC resource must immediately change his/her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

5.2.3. ITC resources are required to notify IT Services and any other user whose password has been revealed or compromised.

5.2.4. Passwords issued by a security administrator must be expired, forcing the user to choose another password before the logon process is completed where possible.

5.2.5. Passwords that are inadvertently revealed are to be changed immediately.

5.2.6. If an ITC resource's password is demanded by anyone, refer them to this document; have them contact the Director, Information Technology Services or your supervisor.

5.2.7. ITC resources must not reveal a password on questionnaires or any type of form.

5.2.8. Security administrators must verify the ID of the ITC resource before resetting any passwords.

5.2.9. ITC resources must not store fixed passwords in Internet browsers; nor in unsecured and unrestricted dial-up communication programs or related data communications software at any time.

5.2.10. Substation cyber assets passwords are contained within Asset Sentry as the exclusive Password Vault for such information. Refer to section 5.4.

5.3. ITC CORPORATE NETWORK SPECIFIC STANDARDS

5.3.1. ITC resources must employ strong passwords of at least 8 characters in length and must contain at least three of the following four character groups: (C7R5.3.1

5.3.1.1. Upper case alphabetic characters.

5.3.1.2. Lower case alphabetic characters.

5.3.1.3. One special character.

5.3.1.4. One numeric character.

5.3.2. ITC enforces a minimum password age of ten days. Once a password is reset for an ITC Resource they cannot change it for ten days. Password can be reset by IT Services within those ten days.(C7R5.3.2)

5.3.3. Corporate systems must be configured to mandate password changes with a frequency not to exceed sixty (60) days. (C7R5.3.3)

5.3.4. ITC corporate networks allow a maximum of three (3) incorrect logon attempts, after which the user will be locked out and be required to contact information services to clear the lockout.

5.3.5. When an ITC resource with Domain Administrator rights leaves the employment of ITC, all domain passwords will be changed at the time their rights have been revoked.

5.3.6. Service account passwords that initiate a service for an application to start do not require the password to be changed at all due to the nature of a service account.

5.3.7. All service account passwords will be stored in a secure password database.

5.3.8. Controls to prevent a user from using a service account.to login are required.

5.4. ASSET SENTRY SPECIFIC PASSWORDS

5.4.1. Asset Sentry user must employ their ITC Active Directory given user name and password for access. Refer to section 5.3 for guidelines. (C7R5.3.2)

5.4.2. Asset Sentry systems are linked to ITC's Active Directory for user access control. (C7R5.3.3)

5.4.3. Asset Sentry contains layers of privileges pertaining to applications, administration, data management and information classification. Access of any level must be restricted and only granted with approval by the Director of Asset Management.

5.4.4. All passwords for Substation Cyber Assets deemed Critical Cyber Assets per NERC CIP-002 standard must be reset at least annually.

5.4.5. Passwords for a Substation Critical Cyber Asset must be device specific, strong, unique and randomly generated while following CIP-007 R 5.3.

5.5. TMS SPECIFIC STANDARDS

5.5.1. General TMS user access to the TMS applications is through a virtual PC that shall have a strong password (8 character minimum, 1 capital letter, 1 lower case letter, 1 special character and 1 number). The virtual PC passwords shall be changed every 60 days. (C7R5.3.2)

5.5.2. Operations and TMS support TMS users have access to the TMS applications through physical PC workstations in the TMS PSPs. These workstations shall have strong passwords (8 character minimum, 1 capital letter, 1 lower case letter, 1 special character and 1 number). The passwords shall be changed twice per year. (C7R5.3.3)

5.5.3. TMS application WS500 accounts shall have a strong password (8 characters minimum, 1 capital letter, 1 lower case letter, 1 special character and 1 number). The account passwords shall be changed twice per year.

5.5.4. TMS support admin accounts shall use strong passwords (8 character minimum, 1 capital letter, 1 lower case letter, 1 special character and 1 number). The passwords shall be changed twice per year except for accounts where it is not technically feasible.

5.6. PEOPLESOFT SPECIFIC STANDARDS

5.6.1. PeopleSoft passwords must be a minimum of eight (8) characters in length and contain one numeric character and one special character.

5.6.2. The maximum allowed incorrect logon attempts into the PeopleSoft application is three (5).

5.6.3. PeopleSoft users are prevented from reusing the previous twelve (12) passwords.

5.6.4. PeopleSoft will mandate password changes with a frequency not to exceed sixty (90) days. Users will automatically be notified fourteen (14) days prior to password expiration.

5.7. POWERPLANT SPECIFIC STANDARDS

5.7.1. Power Plant passwords should be a minimum of eight (8) characters in length and contain one numeric character. Special characters are not required, but are allowed.

5.7.2. The PowerPlant application allows a maximum of three (3) incorrect logon attempts, after which the user will be locked out and be required to contact information services to clear the lockout.

5.7.3. PowerPlant passwords expire every sixty (90) days.

5.8. TRANSMISSION OPERATION DATA SYSTEMS (TODS) SPECIFIC STANDARDS

5.8.1. TODS Forms Users must employ strong passwords of at least eight (8) characters in length, should not contain the account name and must contain at least 3 of the following 4 character groups:

5.8.1.1 Upper case alphabetic characters.

5.8.1.2 Lower case alphabetic characters.

5.8.1.3 One special character.

5.8.1.4 One numeric character.

5.8.2. TODS Forms must be configured to mandate password changes with a frequency not to exceed sixty (60) days. Once a password is reset the prior password cannot be reused until the passwords have been changed four (4) times and forty (40) days has transpired since last use.

5.8.3. TODS FORMS shall allow a maximum of three (3) incorrect logon attempts, after which the user will be locked out and be required to contact TODS_SUPPORT to clear the lockout.

6. ATTACHMENTS

6.1. CIP-024-Att99 Annual Review Internal -Attachment 99

7. MISCELLANEOUS

7.1. N/A

8. APPROVALS

Owner: <Signature on file> Date: 03/26/2012

Approver: <Signature on file> Date: 03/26/2012

9. REVISION HISTORY

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
06/25/2008	000	M. Pokas	Created in accordance with NERC Standard CIP-007 Requirement R1 and R5.3.
04/29/2009	001	L. Trammer	Added 5.1.5 and changed from SSE to CIP
06/24/2009	002	M. Pokas/ M. Ensink	Changes due to annual review. Changed IT Support to IT Services. Added 5.3.2. Changed 1.2 for attachment 99, updated references and attachments.
06/30/2009	003	D. DesRosiers	.Added Section 5.5.4.
10/28/2009	004	A. Stefan	Added section 5.8

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
04/07/10	005	M. Pokas/M. Ensink/P. Melendez	Section 1.2: Replaced "periodically" with "annually". Section 5.3.1 changed - passwords must have 1 of all of the character types listed. Section 5.5 (5.5.1 thru 5.5.4): Updated TMS Specific Standards section to reflect TMS application specific passwords. Section 6.1: Added "tt" to A"tt"99. Updated sub-section of Section 1.2 by removing reference to CIP-003 R1 statement and CIP-007 R1 (not applicable). Updated the now section 1.2.1 by adding "and its sub-requirements". Removed reference to CIP-003 NERC standard from Section 3 and updated CIP-007 reference with Standard name. Section 5.1.1 updated to state resource use in production. Added "your supervisor" to Section 5.2.6. Enhanced wording of section 5.2.9 for systems password storage. Added Section 5.2.10 Asset Sentry password vault Standard. Revised 5.4 to address the use of Active directory for Asset Access and Substation Cyber Assets password statements.
06/30/10	006	M. Ensink	Section 5.3.1 – changed because passwords can have 3 of the 4 character groups, all of the four is not feasible.

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
03/30/11	007	C. Lewis	Changed Mike Pokas' title throughout to Director, Information Technology Services. Added Section .5.3.8. Controls to prevent a user from using a service account.to login are required. Changed 5.4.5.**To** Passwords for configuration of a Substation Critical Cyber Asset must be device specific, strong, unique and randomly generated while following CIP-007 R 5.3. **From**… Passwords for configuration of a Substation Critical Cyber Asset must be device specific, strong, unique and randomly generated while following ITC's standard described in section 5.3.1.
03/28/12	008	J. Sanford M. Pokas P. Melendez	Removed Beth Howell and Steve Stout as approvers. Added Standard references. Removed "configuration of…" from section 5.4.5. Password requirements apply to all.