Standard CIP-003-1
System Management Controls
Disclaimer

This NPCC TFIST workshop provides a forum for the presentation and discussion of member experience in the implementation of compliance programs for the NERC CIP Cyber Security Standards. Materials presented or discussed are the presenters’ own interpretation and recommendations and do not necessarily represent those of their organizations or NPCC.
CIP-003 Purpose

Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
CIP-003 Standard Requirements

- R1 – Cyber Security Policy
- R2 – Leadership
- R3 – Exceptions
- R4 – Information Protection
- R5 – Access Control
- R6 – Change Control and Configuration Management
The Responsible Entity shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
CIP-003 R1 – Cyber Security Policy

- Addresses the requirements in Standards CIP-002 through CIP-009, including provisions for emergency situations.
- The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
- Annual review and approval by Senior Manager assigned (see R2).
CIP-003 R2 – Leadership

- Assign a senior manager with overall responsibility for leading and managing CIP 002-009 implementation and compliance.
  - Identified by name, title, business phone, business address, date of designation
  - Changes to senior management assignee to be documented within 30 days of change
  - Senior management or delegate(s) shall authorize and document any exception from the requirements of the cyber security policy

May 15, 2008
CIP-003 R3 – Exceptions

- Instance where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by CIP Leader or delegate
  - Must be documented within 30 days of being approved by CIP Leader or delegate
  - Documentation must include
    - Why it is necessary and compensating measures
    - OR statement accepting risk
  - Annual review/approval by CIP Leader or delegate to ensure exceptions still valid

May 15, 2008
CIP-003 R4 – Information Protection

- Implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets
- Operational procedures, lists (CIP-002), network topology, floor plans, equipment layouts, DR plans, incident response plans, security configuration—at a minimum
- Classify based on sensitivity
- Yearly assessment, document results, action plan for remediation (based on assessment)
CIP-003 R5 – Access Control

- Document and implement a program for managing access to protected CCA information
- Maintain list of personnel that authorize logical or physical access to protected information
- Annual review of
  - list, access privileges, access control
CIP-003 R6 – Change Control/Configuration Management

- Establish/document process for adding/modifying/replacing/removing CCA hardware/software
- Implement supporting activities to identify/control/document all entity/vendor changes to hardware/software components of CCAs