

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-2
3. **Purpose:** Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-003-2, “Responsible Entity” shall mean:
 - 4.1.1 Reliability Coordinator.
 - 4.1.2 Balancing Authority.
 - 4.1.3 Interchange Authority.
 - 4.1.4 Transmission Service Provider.
 - 4.1.5 Transmission Owner.
 - 4.1.6 Transmission Operator.
 - 4.1.7 Generator Owner.
 - 4.1.8 Generator Operator.
 - 4.1.9 Load Serving Entity.
 - 4.1.10 NERC.
 - 4.1.11 Regional Entity.
 - 4.2. The following are exempt from Standard CIP-003-2:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.
5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

- R1. Cyber Security Policy — 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:
 - R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

- R5.1.2.** The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
- R5.2.** The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
- R5.3.** The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.
- R6.** Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

- M1.** The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.
- M2.** The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.
- M5.** The Responsible Entity shall make available its access control documentation as specified in Requirement R5.
- M6.** The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- 1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.
- 1.1.2** ERO for Regional Entity.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

- Compliance Audits
- Self-Certifications

- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Data Retention

- 1.4.1** The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

- 1.5.1** None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
2	05/06/09	Adopted by NERC Board of Trustees	Revised