NERC CIP: Fundamental Security Requirements of an Electronic Access Control and Monitoring System (EACMS) – Requirements Mapping to ConsoleWorks®

NERC Standard	Requirement		Requirement Text	Measures	ConsoleWorks Solution
CIP-002 Cyber Security - Critical Cyber Asset Identification	R1 - Critical Asset Identification	R1	The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.	The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.	• Reporting - ConsoleWorks Configuration Reporting

CIP-002 Cyber Security - Critical Cyber Asset Identification	R2 – Cyber System Categorization	R2	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.	The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.	• Reporting - ConsoleWorks Configuration Reporting

CIP-003 Cyber Security - Security Management Controls	R4 - Information Protection	R4.1	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	The Responsible Entity shall make available its access control documentation as specified in Requirement R4.	• Security Policy Enforcement
CIP-003 Cyber Security - Security Management Controls	R5 - Access Control	R5.1	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	The Responsible Entity shall make available its access control documentation as specified in Requirement R5.	• Security Policy Enforcement
CIP-003 Cyber Security - Security Management Controls	R6 - Change Control and Configuration Management	R6	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.	The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.	• Reporting - Asset Configuration Reporting • Reporting - Session Reporting • Logging - User Activity • Baseline Configuration Management - Collection of Configuration
CIP-004 Cyber Security - Personnel and Training	R4 - Access	R4	The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.	• Access Management - Role-based Access Control • Reporting - ConsoleWorks Configuration Reporting • Security Policy Enforcement

CIP-005 Cyber Security - Electronic Security Perimeter(s)	R1 - Electronic Security Perimeter	R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.	• Access Management - Role-based Access Control • Access Management - Remote Access Control • Security Policy Enforcement
		R1.6	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.		• Reporting – ConsoleWorks • Configuration Reporting
CIP-005 Cyber Security - Electronic Security Perimeter(s)	R2 - Electronic Access Controls	R2.1	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.	• Access Management - Role-based Access Control • Access Management - Default Deny • Security Policy Enforcement
		R2.3	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).		• Access Management - Remote Access Control
		R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.		• Access Management - Role-based Access Control • Access Management - Remote Access Control

		R2.6	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.		• Security Policy Enforcement
CIP-005 Cyber Security - Electronic Security Perimeter(s)	R3 - Monitoring Electronic Access	R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.	• Access Management - Remote Access Control
		R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety-calendar days.		• Event Management - Real-time Detection • Event Management – Alerts • Correlation - Repeated Security Events • Reporting - Event Reporting • Logging - User Activity in ConsoleWorks • Security Policy Enforcement
CIP-006 Cyber Security - Physical Security	R2 - Protection of Physical Access Control Systems	R2.2	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.	• Security Policy Enforcement

CIP-006 Cyber Security - Physical Security	R6 - Logging Physical Access	R6	Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.	• Logging - Event Logging • Security Policy Enforcement
CIP-007 Cyber Security - Systems Security Management	R1 - Test Procedures	R1.3	The Responsible Entity shall document test results. [Regarding changes to existing Cyber Assets such as patches, service packs, upgrades, etc. as defined in R1.]	The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.	• Logging - User Console Activity
CIP-007 Cyber Security - Systems Security Management	R3 - Security Patch Management	R3.2	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.	• Logging - User Console Activity

CIP-007 Cyber Security - Systems Security Management	R4 - Malicious Software Prevention	R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.	• Logging - Event Logging
CIP-007 Cyber Security - Systems Security Management	R5 - Account Management	R5	The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	The Responsible Entity shall make available documentation and records of its security status-monitoring program as specified in Requirement R6.	• Access Management - Role-based Access Control • Access Management - Remote Access Control • Security Policy Enforcement
		R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.		• Logging - User Console Activity
		R5.2	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.		• Access Management - Role-based Access Control • Access Management - Remote Access Control • Access Management - Command Control • Access Management - Least Privilege Access • Access Management - Default Deny • Reporting – ConsoleWorks • Configuration Reporting • Security Policy Enforcement

		R5.3	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible: R5.3.1. Each password shall be a minimum of six characters. R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters. R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.		• Access Management - Password Management • Security Policy Enforcement
CIP-007 Cyber Security - Systems Security Management	R6 - Security Status Monitoring	R6	The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	The Responsible Entity shall make available documentation and records of its security status-monitoring program as specified in Requirement R6.	• Event Management - Real-time Detection • Correlation - Repeated Security Events • Security Policy Enforcement
		R6.2	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.		• Event Management - Alerts
		R6.4	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.		• Logging - Event Logging
		R6.5	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.		• Reporting - Regulatory Reporting • Reporting - Security Reporting • Reporting - Event Reporting
CIP-007 Cyber Security - Systems Security Management	R7 - Disposal or Redeployment	R7.3	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in	• Logging - User Console Activity

				Requirement R7.	
CIP-007 Cyber Security - Systems Security Management	R8 - Cyber Vulnerability Assessment	R8.3	The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following: [R8.1, R8.2] AND A review of controls for default accounts; and [R8.4]	The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.	• Reporting - ConsoleWorks Configuration Reporting
CIP-008 Cyber Security - Incident Reporting and Response Planning	R1 - Cyber Security Incident Response Plan	R1.1	The Cyber Security Incident response plan shall address, at a minimum, the following: R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.	The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.	• Event Management - Real-time Detection • Event Management - Vendor-specified Event Definitions • Event Management – Correlation • Reporting - Event Reporting
CIP-008 Cyber Security - Incident Reporting and Response Planning	R2 - Cyber Security Incident Documentation	R2	The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	The Responsible Entity shall make available all documentation as specified in Requirement R2.	• Reporting - Security Reporting • Logging - User Console Activity • Logging - Event Logging
CIP-010 Cyber Security - Configuration Change Management and Vulnerability	R1 - Configuration Change Management	R1	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R1 – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	Examples of evidence may include, but are not limited to: A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; OR A record in an asset management system that identifies the required	• Baseline Configuration Management - Collect Configuration • Reporting - Asset Configuration Reporting • Reporting - Audit Reporting

		R1.1	Develop a baseline configuration, individually or by group, which shall include the following items:	items of the baseline configuration for each Cyber Asset, individually or by group.	
		R1.1.1	Operating system(s) (including version) or firmware where no independent operating system exists;		
		R1.1.2	Any commercially available or open-source application software (including version) intentionally installed;		
		R1.1.3	Any custom software installed;		
		R1.1.4	Any logical network accessible ports; and		
		R1.1.5	Any security patches applied		
		R1.2	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; OR Documentation that the change was performed in accordance with the requirement.	• Baseline Configuration Management - Collect Configuration • Baseline Configuration Management - Check Configuration • Event Management - Automated Response Actions • Reporting - Asset Configuration Reporting • Reporting - Audit Reporting
		R1.3	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.	• Baseline Configuration Management - Collect Configuration • Event Management - Automated Response Actions • Reporting - Audit Reporting • Logging - User Activity

		R1.4	For a change that deviates from the existing baseline configuration:	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.	• Reporting - Asset Configuration Reporting • Reporting - Audit Reporting
		R1.4.1	Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;		
		R1.4.2	Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and		
		R1.4.3	Document the results of the verification.		
		R1.5	Where technically feasible, for each change that deviates from the existing baseline configuration:	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.	• Reporting - Asset Configuration Reporting • Reporting - Audit Reporting • Baseline Configuration Management - Compare Multiple Baselines
		R1.5.1	Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and		
		R1.5.2	Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.		

CIP-010 Cyber Security - Configuration Change Management and Vulnerability	R2 - Configuration Monitoring	R2	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.	• Baseline Configuration Management - Collect Configuration • Baseline Configuration Management - Check Configuration • Baseline Configuration Management - Repair Configuration • Baseline Configuration Management - Compare Multiple Configurations • Event Management - Automatic Response Actions
		R2.1	Monitor at least once every 35-calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.		• Baseline Configuration Management - Collect Configuration • Baseline Configuration Management - Compare Multiple Configurations • Event Management - Automatic Response Actions