



EnterpriseSERVER™ Critical Infrastructure Protection Compliance Table

CIP Requirements: Auditing

Standard	Requirement(R#) / Measure(M#) / Compliance#	Description	How EnterpriseSERVER™ addresses this standard
CIP-003-1	Compliance 1.2.	"1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year."	Archive your detailed Audit trails for any required timeframe.
CIP-005-1	R5./M5.	"Monitoring Electronic Access Control - The Responsible Entity shall implement the organizational, technical and procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized access to the electronic perimeter(s) and Critical Cyber Assets within the perimeter(s), 24 hours a day, 7 days a week."	Administrators can connect to other users' sessions to monitor their activities & take control of their sessions. Audit trails of who accessed what device at what time. Intrusion detection through audit logs.
CIP-007-1	R7.1./M6.	"The Responsible Entity shall retain said log data for a period of ninety (90) calendar days."	Archive your detailed Audit trails for any required timeframe.
CIP-007-1	R7.	"Retention of Systems Logs: Using monitoring systems and/or procedures either internal and/or external to Critical Cyber Assets, the Responsible Entity shall ensure it is possible to create an audit trail from logs of security-related events affecting the Critical Cyber Assets. The Responsible Entity must determine its own logging strategy to fulfill the requirement."	Audit trails are enabled by default with EnterpriseSERVER, it is also possible to record all actions taken by a user if required.
CIP-008-1	M2.	"The Responsible Entity shall retain records in addition to requirements defined in Standard CIP-007-1, requirement R7 (Retention of Systems Logs) of Cyber Security Incidents for three calendar years."	Archive your detailed Audit trails for any required timeframe.



EnterpriseSERVER™ Critical Infrastructure Protection Compliance Table

CIP Requirements: Electronic Security Perimeter

Standard	Requirement(R#) / Measure(M#) / Compliance#	Description	How EnterpriseSERVER™ addresses this standard
CIP-005-1	R4.2.	"Where external interactive logical access to the electronic access points into the Electronic Security Perimeter is implemented, the Responsible Entity shall implement strong procedural or technical measures to ensure authenticity of the accessing party. These strong procedural or technical measures shall include at least one of the following measures: -Two-factor authentication -Digital certificates "	EnterpriseSERVER uses RSA SecureID cards, or digital certificates (what you have) in combination with STRONG passwords (what you know) to achieve secure, two-factor authentication to meet these requirements.
CIP-005-1	R4.2.	"In dial-up access, call back to augment static user id and password authentication"	Use of dial-back modems, modem banks, complex (STRONG) passwords on EnterpriseSERVER ensure that unwanted intruders are explicitly denied access through dial-up connections.
CIP-005-1	R4.1.	"These Electronic Security Perimeter access controls shall implement an access control model, which denies access by default unless explicit access permissions are specified."	Access control is done through one interface screen on the EnterpriseSERVER machine. Delegate user/group access on proven Windows Server technologies.
CIP-005-1	R4./M4.	"Electronic Access Controls - The Responsible Entity shall implement the organizational, technical and procedural controls to permit or deny logical access at all electronic access points to the Electronic Security Perimeter(s) and the Critical Cyber Assets within the Electronic Security Perimeter(s)."	EnterpriseSERVER forces all users to authenticate through one single point of access, making the task of allowing or denying user access to your substation devices simple to administer.
CIP-005-1	R3./M3.	"The Responsible Entity shall secure dial-up modem connections. Where remote activation of dial-up connectivity via SCADA activated relays from the security or control center is technically feasible, dial-up equipment at unattended facilities shall be physically deactivated when not in approved use and remotely activated upon approval of activation. In all other cases, the Responsible Entity shall implement procedural or technical measures to ensure authenticity of the accessing device and/or application."	Use of dial-back modems, modem banks on EnterpriseSERVER ensure that unwanted intruders are explicitly denied access through dial-up modems.
CIP-005-1	R2./M2.	"Disabling unused Network Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other Ports/Services, including those used for testing purposes, must be disabled prior to production usage."	A lockdown utility is used to close all unnecessary ports, disable unused guest accounts etc. prior to going live.
CIP-005-1	R1./M1.	"Electronic Security Perimeter - The Electronic Security Perimeter is the logical border surrounding the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled. The Responsible Entity shall identify the Electronic Security Perimeter(s) surrounding its Critical Cyber Assets and all access points to the perimeter(s). Access points to the Electronic Security Perimeter(s) shall additionally include any externally connected communication end point (e.g. modems) terminating at any device within the Electronic Security Perimeter. Communication links connecting discrete electronic perimeters are not considered part of the security perimeter. However, end-points of these communication links within the security perimeter(s) are considered access points to the Electronic Security Perimeter(s). Where there are also non-Critical Cyber Assets within the defined Electronic Security Perimeter, these non-Critical Cyber Assets must comply with the requirements of this standard."	A network "Electronic Security Perimeter" diagram is prepared prior to installation of EnterpriseSERVER for clarification and understanding of how the solution best suits your organization. Vulnerabilities will be addressed, your substation network will be analyzed and improvements will be made where seen fit prior to implementation.
CIP-007-1	R9./M8.	"Disabling Unused Host Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage."	A lockdown utility is used to close all unnecessary ports, disable unused guest accounts etc. prior to going live.
CIP-007-1	R5.1./M4.	"The Responsible Entity shall use Integrity Software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer), to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (mal-ware) to other Cyber Assets within the Electronic Security Perimeter."	Symantec Antivirus Corporate Edition is standard with any installation of EnterpriseSERVER, which protects your systems from virii and spyware/malware.



EnterpriseSERVER™ Critical Infrastructure Protection Compliance Table

CIP Requirements: General Policy

Standard	Requirement(R#) / Measure(M#) / Compliance#	Description	How EnterpriseSERVER™ addresses this standard
CIP-003-1	R4. - R5.	"The process should include change management procedures that at a minimum provide testing, modification audit trails, problem identification, a back out and recovery process should modifications fail, and ultimately ensure the overall integrity of the Critical Cyber Assets."	EnterpriseSERVER uses built-in Microsoft Windows Server components, where audit trails, system recovery, and intrusion detection are proven & trusted technologies available to ensure data integrity.
CIP-004-1	M2.1	"The cyber security policy"	EnterpriseSERVER training is provided, covering important security topics such as: potential threats & vulnerabilities, security best practices, social engineering, data integrity & backups, system overview, acceptable usage, guidelines for securing your substation assets.
CIP-004-1	Compliance 1.4.1	"Document(s) for compliance, training, awareness"	EnterpriseSERVER training students receive a Certificate indicating that they have received Security best practices training.
CIP-007-1	R1.	"Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment. All testing shall be performed in a manner that precludes adversely affecting the production system and operation."	EnterpriseSERVER is set up in a controlled lab and tested to meet your requirements, and to comply with security standards, before commissioned in a production environment.
CIP-009-1	R5.	"The Responsible Entity shall develop training and awareness for its recovery plan(s)"	EnterpriseSERVER training is provided, covering important security topics such as: potential threats & vulnerabilities, security best practices, social engineering, data integrity & backups, system overview, acceptable usage, guidelines for securing your substation assets.



EnterpriseSERVER™ Critical Infrastructure Protection Compliance Table

CIP Requirements: Information Management

Standard	Requirement(R#) / Measure(M#) / Compliance#	Description	How EnterpriseSERVER™ addresses this standard
CIP-004-1	M2.4	"Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident."	EnterpriseSERVER training is provided, covering important security topics such as: potential threats & vulnerabilities, security best practices, social engineering, data integrity & backups, system overview, acceptable usage, guidelines for
CIP-004-1	M2.3	"The proper release of Critical Cyber Asset information;"	



EnterpriseSERVER™ Critical Infrastructure Protection Compliance Table

CIP Requirements: Roles & Responsibilities

Standard	Requirement(R#) / Measure(M#) / Compliance#	Description	How EnterpriseSERVER™ addresses this standard
CIP-003-1	R4. - R4.	"The approving authority shall be responsible for verifying that a system meets minimal security configuration standards prior to the system being promoted to operate in a production environment."	EnterpriseSERVER is set up in a controlled lab and tested to meet your requirements, and to comply with security standards, before commissioned in a production environment.
CIP-003-1	R3.	"The Responsible Entity shall also define the roles and responsibilities of Critical Cyber Asset owners, custodians, and users. Roles and responsibilities shall also be defined for the access, use, and handling of critical information..."	An essential security measure, EnterpriseSERVER requires strict definition of roles & responsibilities and group membership based on required levels of user access.
CIP-003-1	M12.	"The Responsible Entity shall review the roles and responsibilities of Critical Cyber Asset owners, custodians, and users at least annually."	Individual user accounts can be set to expire on a schedule, requiring a re-evaluation of user roles on your pre-defined dates.
CIP-004-1	R2./M2.	"Training - The Responsible Entity shall develop and maintain a company specific cybersecurity-training program that will be reviewed annually. This program will ensure that all personnel having authorized access to Critical Cyber Assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these Critical Assets."	EnterpriseSERVER training is provided, covering important security topics such as: potential threats & vulnerabilities, security best practices, social engineering, data integrity & backups, system overview, acceptable usage, guidelines for securing your substation assets.
CIP-004-1	R1./M1.	"Awareness - The Responsible Entity shall develop, maintain and document its security awareness program to ensure personnel subject to the standard receive on-going reinforcement in sound security practices."	
CIP-004-1	Compliance 1.4.4	"Verification that quarterly and annual security awareness have been conducted"	EnterpriseSERVER training students receive a Certificate indicating that they have received Security best practices training.
CIP-007-1	R6.1./M5.	"The Responsible Entity shall perform a vulnerability assessment at least annually that includes: R6.1.1. A diagnostic review of the access points to the Electronic Security Perimeter R6.1.2. Scanning for open ports/services and modems R6.1.3. Factory default accounts R6.1.4. Security patch and anti-virus version levels"	Prior to EnterpriseSERVER installation, an assessment is conducted on the architecture of your substation network to mitigate the possibility of intrusions. All vulnerabilities will be reported and recommendations given. Post-installation, we recommend a third party to perform a yearly vulnerability assessment.
CIP-007-1	R4.1./M3.	"The Responsible Entity shall evaluate all patches and upgrades for applicability to the individual situation, e.g. using a risk based assessment, so as to avoid un-necessary and excessive patching."	Use of a free tool from Microsoft is installed with EnterpriseSERVER, which enables administrators to first review a patch, test it, and then deploy it on clients to ensure uptime while updating systems with the latest security patches.
CIP-007-1	R4./M3.	"Security Patch Management: The Responsible Entity shall establish a formal security patch management program for tracking, evaluating, testing, and installation of applicable security patches and upgrades to critical cyber security assets."	
CIP-007-1	R3.4.	"Access Reviews - Attended: The Responsible Entity shall ensure a designated approver reviews access to Critical Cyber Assets, e.g., computer and/or network accounts and access rights, at least semi-annually. Unauthorized, invalidated, expired, or unused computer and/or network accounts shall be disabled."	This is a security best practices guideline that is easy to accomplish with EnterpriseSERVER in place. All done through one interface.
CIP-007-1	R11./M10.	"Back up and Recovery: The Responsible Entity shall back up on a regular basis, where technically feasible, information and data that is resident or required by Cyber Assets used to manage critical electric infrastructure."	A backup & recovery plan is covered and implemented with EnterpriseSERVER.
CIP-007-1	R10./M9.	"Operating Status Monitoring Tools: For maintaining situational awareness, the Responsible Entity shall ensure Critical Cyber Assets used for operating critical infrastructure are included or augmented with automated and/or process tools, where practical, to monitor operating state, utilization and performance, and cyber security events experienced by the Critical Cyber Assets themselves, and issue alarms for specified indications, as implemented."	Industry-leading Windows Server built in performance monitoring components are available in conjunction with auditing capabilities to conform to this standard.



EnterpriseSERVER™ Critical Infrastructure Protection Compliance Table

CIP Requirements: User Access Management

Standard	Requirement(R#) / Measure(M#) / Compliance#	Description	How EnterpriseSERVER™ addresses this standard
CIP-003-1	R8.	"Responsible Entities shall define and document procedures to ensure that modification, suspension, or termination of user access to Critical Cyber Assets is accomplished in a time frame that ensures Critical Cyber Assets are not put at significant risk. All access revocations/changes must be authorized and documented."	Account administration is all done through one simple screen, using built-in Windows Server technologies.
CIP-003-1	R7.	"Responsible Entities shall review access rights to Critical Cyber Assets to confirm they are correct and that they correspond with the entity's needs and the appropriate roles and responsibilities."	The EnterpriseSERVER interface makes the process of reviewing user/group roles and device privileges a simple task.
CIP-003-1	R5. - R6.	"The Responsible Entity shall maintain a list of personnel who are responsible to authorize access to Critical Cyber Assets."	Quickly generate current lists & reports of users and groups with access to substation devices.
CIP-003-1	R5.	"The Responsible Entity shall institute and document a process for management of access to information associated with Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible."	Management of user access to substation devices is done through a simple interface, on a per-device/per-port level.
CIP-004-1	M4.3	"Physical and electronic access revocation must be completed within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.)."	The EnterpriseSERVER interface makes the process of reviewing user/group roles and device privileges a simple task.
CIP-004-1	M4.1	"Maintain a list of all authorized personnel with access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets within the security perimeter(s)."	Quickly generate current lists & reports of users and groups with access to substation devices.
CIP-004-1	M2.2	"Physical and electronic access controls to Critical Cyber Assets"	EnterpriseSERVER training is provided, covering important security topics such as: potential threats & vulnerabilities, security best practices, social engineering, data integrity & backups, system overview, acceptable usage, guidelines for securing your substation assets.
CIP-005-1	R4.3.	"Where technically feasible, electronic access control devices shall display an appropriate use banner upon interactive access attempts."	Network Policies can be displayed when user first logs in to system to indicate the severity of malicious actions.
CIP-007-1	R3.2.	"Generic Account Management- Attended: The Responsible Entity shall have a process for managing factory default accounts, e.g., administrator or guest. The process shall include the removal, disabling, or renaming of these accounts where possible. For those accounts that must remain, passwords shall be changed prior to putting any system into service. Where technically supported, individual accounts shall be used (in contrast to a group account). Where individual accounts are not supported, the Responsible Entity shall have a policy for managing the appropriate use of group accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of staff changes, e.g., change in assignment or exit."	Unnecessary accounts are disabled, default Windows accounts are disabled where possible, Administrator privileges are granted to a defined users' account and then the Administrator account will be disabled to prevent intrusions. Strict account management is vital to the security of any system.
CIP-007-1	R3.1./M2.	"Strong Passwords: In the absence of more sophisticated authentication methods that are stronger than passwords and don't require a password, (e.g., multi-factor access controls, artifacts, or bio-metric), the Responsible Entity shall use accounts that have a strong password. For example, a password consisting of a combination of alpha, numeric, and special characters with a minimum of six characters to the extent allowed by the existing technology. Passwords shall be changed periodically per a risk-based frequency to reduce the risk of password cracking."	Complex (STRONG) passwords are enabled by default, adhering to this standard. Password expiration is also set prior to production.
CIP-007-1	R3./M2.	"Account and Password Management: The Responsible Entity shall establish an account password management program to provide for access authentication, auditability of user activity, and minimize the risk to unauthorized system access by compromised account passwords."	EnterpriseSERVER forces users to have Complex (STRONG) passwords, 2-factor authentication, all while auditing every action taken during a user session.