

## NERC CIP Security Audit Checklist

### North American Reliability Corp. (NERC) Critical Infrastructure Protection (CIP)

Requirements	Procedures	Status	Notes
Electronic Security (CIP-002, 003, 005, 007, 009)	Maintain an inventory of all electronics that either are part of the critical assets list or are necessary to the operation of critical assets.		
	Protect access to these critical cyber-assets on a need-to-know basis.		
	Create an electronic security perimeter that prevents unauthorized users from accessing any critical cyber-asset, whether they are outside or inside the corporate network.		
	Ensure that all electronic cyber-assets are secure via user account management, equipment, password management, and secure networking policies.		
	Implement and test a critical cyber-asset recovery plan.		
Physical Security (CIP-006)	Ensuring that there is a physical security perimeter around all critical cyber-assets.		
	All physical access points to critical cyberassets must be identified and controlled.		
	An access log must be maintained for all critical cyber-assets, via keycards, video or manual log.		
Personnel Security (CIP-004)	Each person who accesses critical cyberassets, including the utility's personnel, contract workers and vendors, must be investigated to assess the risk that he or she poses to security.		
Training and Awareness (CIP-004)	Everyone who has access to critical cyberassets, including utility personnel, contract workers and vendors, must be trained in cyber-security.		
Audits and Documentation (All CIP standards)	All CIP standards make it mandatory to document and review all procedures and policies every year. NERC will audit compliance on all the standards on a schedule provided by the organization.		
Recovery Plans (CIP-	Backup strategies		
	Data restoration strategies		
	Spare parts and equipment.		