

NERC CIP Compliance

Solution Brief

Critical Infrastructure Protection standards compliance for grid operators and power providers. Claviger implements NERC CIP security controls at the AI governance layer.

Access Controls: NERC CIP requires strict access controls on critical systems. Claviger enforces role-based access policies for AI systems controlling critical assets. Every AI access is logged and cryptographically verified.

Security Event Monitoring: NERC CIP section 6 requires real-time monitoring of critical system events. Claviger logs every governance decision and AI action, creating the event records required by NERC CIP.

Incident Response: When security incidents occur, Claviger provides the immutable evidence needed for incident investigation and remediation verification.

Compliance Auditing: NERC CIP requires demonstration of control effectiveness. Claviger provides cryptographic evidence proving that security controls are functioning as designed.

