Bright Utility Company ARS-CIP Cybersecurity Policy

Version: 1.0
Effective Date: 02/02/2025
Owner: CIO
Last Reviewed: 31/12/2024

1. Purpose

The purpose of this policy is to establish Bright Utility Company's (BUC) Asset & Risk Security – Critical Infrastructure Protection (ARS CIP) compliance framework. This policy ensures that BUC complies with regulatory requirements, including NERC CIP standards, to protect critical infrastructure and maintain operational resilience.

2. Scope

This policy applies to all BUC employees, contractors, and third-party vendors who interact with:

- Critical infrastructure assets within BUC's environment.
- Information security systems supporting ARS CIP compliance.
- Cloud and on-premises environments used for CIP operations
- Audit and compliance processes related to regulatory obligations.

3. Policy Statements

BUC follows a structured compliance framework that includes:

3.1 NERC CIP Compliance

3.1.1. Adhering to CIP-002 to CIP-013 for infrastructure protection.
3.1.2. Implementing strict access controls and authentication policies.
3.1.3. Ensuring incident response and reporting mechanisms.

3.2 Risk Management & Governance

3.2.1. Conducting periodic risk assessments for CIP-related assets.
3.2.2. Defining a risk treatment strategy for identified vulnerabilities.
3.2.3. Integrating Three Lines of Defense (3LoD) risk governance.
3.2.4. Risk assessments will be conducted periodically whenever significant changes to the operational technology systems or business processes occur.

3.3 Audit & Evidence Management

3.3.1. Maintaining audit logs for compliance verification.
3.3.2. Ensuring documentation meets internal and regulatory audit standards.
3.3.3. Conducting annual self-certifications and audits.

3.4 Incident Response

In the event of a security incident affecting critical infrastructure:

3.4.1. Report the incident immediately to the Compliance & IT Security Team.
3.4.2. Activate the incident response plan as per CIP-008-AB guidelines.
3.4.3. Investigate and document the incident following BUC's Root Cause Analysis (RCA) process.
3.4.4. Remediate vulnerabilities and update compliance records accordingly.
3.4.5. All employees and stakeholders will be trained on their roles and responsibilities in the event of a security incident.
3.4.6. Security incidents will be logged, investigated, and reported to the appropriate authorities as required.

3.5 Training and Awareness

3.5.1. Annual ARS CIP training for all personnel handling CIP assets
3.5.2. Quarterly awareness campaigns on compliance risks and best practices
3.5.3. Tabletop exercises and simulations for incident response preparedness.
3.5.4. Phishing simulations and other awareness activities will be carried out to reinforce security awareness.

4. Compliance and Enforcement

Failure to comply with this policy may result in:

4.1.1. Corrective actions, including mandatory retraining.
4.1.2. Internal disciplinary actions, depending on the severity of non-compliance.
4.1.3. Regulatory fines or penalties, if violations lead to external compliance breaches

The CIO will ensure that this policy is reviewed and updated regularly to reflect changes in the CIP cybersecurity landscape and business requirements.

5. Policy Review

This policy is subject to review annually or in response to significant regulatory changes. The Compliance Team is responsible for ensuring the policy remains aligned with NERC CIP and BUC's risk management strategy.

6. Roles and Responsibilities

Role	Responsibility
Compliance Team	Maintain policies, conduct risk assessments, and manage audits
IT Security	Implement security controls for infrastructure protection.
Risk Management	Identify, assess, and mitigate compliance risks.
Audit Team	Ensure adherence to ARS CIP and other regulatory requirements.
Business Units	Follow compliance policies and report security concerns.

Next Review Date: 31/12/2025
Approved by:
Chief Information Officer (CIO)
Date: 31/01/2025