

TXNM ENERGY, INC.
BOARD OF DIRECTORS
CYBER RISK POLICY
APPROVED MARCH 1, 2022

BACKGROUND

The Board of Directors (the “Board”) of TXNM Energy, Inc. (the “Company”) has determined that it is in the best interests of the Company and its shareholders to adopt this Cyber Risk Policy (the “Policy”). This Policy is effective as of March 1, 2022.

The Company believes that cyber risk, like safety, is everyone’s responsibility. The Company is committed to a Simplify, Standardize, and Secure by making systems Resilient, Redundant and Reliable cyber risk philosophy. A core principle of this philosophy is that only by simplifying and standardizing the Company’s systems and services can the Company be able to secure them, and only by ensuring their redundancy and resilience, can the Company provide a reliable electric supply. In order to implement this philosophy, the Company maintains a robust, enterprise-wide, risk-based security program, informed by the National Institute of Science and Technology Cybersecurity Framework for Protecting Critical Infrastructure. To protect its most critical systems, the Company also complies with the North American Electric Reliability Corporation’s Critical Infrastructure Protection Standards. This philosophy, guided by these standards provides a framework for managing cybersecurity risk.

The Board therefore has adopted this Policy to enhance its understanding and oversight of the policies, controls and procedures that have been put in place to (i) identify, manage and mitigate risks related to cyber risk; and (ii) respond to incidents with respect thereto. The Audit Committee of the Board (the “Audit Committee”) oversees this Policy for the Board. The Audit Committee’s oversight of cyber risk management will assist in the Board’s assessment of the adequacy of resources, funding, and focus within the Company with respect to cyber risk.

POLICY

1. Management shall provide regular reports to the Audit Committee and, if requested, to the Board on the status and progress of the Company’s cyber risk program, including:
 - a. Information and data security systems and controls designed to identify, protect, detect, respond to and recover from cyber risk vulnerabilities, cyber-attacks or breaches;
 - b. cyber risk program budget and staffing;
 - c. Crisis Management, incident response plan and disaster recovery capabilities, including participating in periodic “tabletop” exercises simulating cyber risk scenarios; and
 - d. Trends, developments and best practices in cyber risk and data security.
2. The Audit Committee shall periodically review with management the Company’s management of risks and compliance with legal and regulatory requirements and industry standards related

to its information technology security systems and processes, including network security and data protection. The Audit Committee shall, when appropriate, review and discuss with management summaries of findings from completed internal audits of such systems and processes and discuss the same when appropriate with the internal auditor.

3. The Company shall periodically assess its vulnerability to cyber-attack by employing when appropriate third-party audits, penetration tests, and internal process assessments to continuously improve its internal cyber risk and data privacy controls.
4. The Company shall partner with government and industry peers in appropriate cyber risk programs to share information and provide mutual assistance in the event of a cyber-attack.
5. The Company shall assess the risk of third-party suppliers as part of its procurement process and incorporate appropriate cyber risk controls in supplier contracts and, at the Company's discretion, audit suppliers to ensure adherence to those controls.
6. Management shall increase cyber risk awareness within the Company and implement when appropriate additional technologies to enhance its cyber risk capabilities.
7. The Board may amend this Policy in its sole discretion from time to time and for any reason, including to comply with the requirements of any forthcoming regulations. The Board may terminate this Policy at any time.