4 RIVERS ELECTRIC COOPERATIVE, INC.
LEBO, KANSAS

Board of Trustees Policy

Subject: **Cybersecurity & Data Governance**			Policy No: **303**
Original Issue: 10/20/2025	Last Revised: 10/20/2025	Last Reviewed: 10/20/2025	Page 1 of 2

I. OBJECTIVE

To establish the 4 Rivers Electric Cooperative, Inc.'s (Cooperative's) Board of Trustees' expectations regarding the protection of the Cooperative's digital systems, technology infrastructure, and information assets, including member, employee, and operational data. The purpose of this policy is to ensure responsible stewardship, safeguard Cooperative operations from cyber-related threats, and maintain trust, continuity, and data integrity.

II. POLICY

A. The Board of Trustees recognizes that information, data systems, and technology infrastructure are assets of the Cooperative and must be protected with the same diligence applied to physical and financial assets.

B. Cybersecurity, data privacy, and protection of information systems are matters of governance oversight. The Cooperative shall exercise sound judgment, reasonable security practices, and due care in preventing unauthorized access, use, alteration, disclosure, or destruction of Cooperative assets or data.

C. The Cooperative shall maintain reasonable safeguards to protect against internal and external threats, including but not limited to cyberattacks, unauthorized system access, data loss, and technology-related disruptions.

D. The General Manager/CEO (CEO) shall establish and maintain procedures to:

1. Control access to Cooperative technology systems and data;
2. Establish authentication and credential management standards;
3. Govern acceptable use of Cooperative technology resources;
4. Detect and respond to cybersecurity incidents or attempted intrusion;
5. Train employees on responsible data handling and cybersecurity awareness;
6. Implement appropriate data backup, storage integrity, and recovery practices;

7. Evaluate vendor and third-party access to Cooperative systems when applicable.

E. The CEO shall ensure that procedures are reviewed periodically and adjusted to address evolving risks, industry standards, insurance requirements, and technological changes.

F. Significant cybersecurity incidents that could materially impact Cooperative operations, financial standing, or member confidence shall be reported to the Board of Trustees in a timely manner.

III. ADMINISTRATION

A. The CEO is responsible for developing, implementing, and maintaining administrative procedures consistent with this policy and for ensuring that Cooperative personnel comply with established cybersecurity and data governance practices.

IV. RESPONSIBILITY

A. The Board of Trustees is responsible for the oversight of this policy. The CEO is responsible for its administration and for implementing appropriate safeguards to protect Cooperative systems, data, and digital infrastructure.

10/20/2025
Date

/s/ Warren Schmidt
Board of Trustees, Secretary