RESOLUTION NO. 25-002

A RESOLUTION OF THE BOARD OF DIRECTORS OF CALIFORNIA ELECTRONIC RECORDING TRANSACTION NETWORK AUTHORITY (CeRTNA) ADOPTING A CYBERSECURITY TRAINING POLICY

25-002.1 Purpose: The purpose of this policy is to ensure that all employees and contractors are provided with the necessary training to recognize, avoid, and respond to cybersecurity threats, thereby protecting the organization's assets, data, and systems from unauthorized access, breaches, and other cybersecurity risks.

25-002.2 Scope: This policy applies to all employees, contractors, and third-party vendors who have access to the organization's network, systems, or data. All individuals covered under this policy are required to complete cybersecurity training to ensure compliance with organizational security standards and regulatory requirements.

25-002.3 Policy Statement: Cybersecurity is a shared responsibility that requires consistent and ongoing training. The organization is committed to providing comprehensive cybersecurity training to ensure all employees understand how to protect sensitive information, recognize threats, and follow security best practices. Regular cybersecurity training sessions will be held to mitigate the risk of cyber incidents and ensure that staff are well-equipped to respond effectively to evolving security challenges.

25-002.4 Training Requirements:

- **New Employees:** All new employees will complete mandatory cybersecurity training during their onboarding process. This training must be completed within the first 30 days of employment.
- **Annual Training:** All employees and contractors must complete cybersecurity training annually. The training will be updated regularly to address new and emerging threats.
- **Specialized Training:** Employees in roles with elevated access or responsibility over sensitive information (e.g., IT, finance, HR) will receive additional role-specific cybersecurity training tailored to the risks associated with their position.
- **Third-Parties:** All vendors and contractors with access to the organization's systems and data must complete cybersecurity awareness training as part of their contractual agreements.

25-002.5 Training Content:

Cybersecurity training will include, but is not limited to, the following topics:

- **Password Security and Management:** Best practices for creating, managing, and safeguarding passwords.
- **Recognizing Phishing and Social Engineering Attacks:** How to identify fraudulent emails, phone calls, and other social engineering attacks.
- **Data Protection and Privacy:** Handling sensitive information, ensuring confidentiality, and understanding data privacy regulations (such as GDPR, CCPA, etc.).
- **Incident Response Procedures:** Steps to take if a cyber incident is suspected or confirmed.
- **Safe Internet and Email Use:** Guidelines for secure web browsing, email usage, and preventing malware infections.
- **Remote Work Security:** Best practices for securing devices and networks when working remotely.
- **Device Management:** Guidelines on securing mobile and personal devices used for work purposes.

25-002.6 Responsibility:

- **Executive Director:** Responsible for creating, updating, and delivering cybersecurity training, as well as monitoring compliance with this policy.
- **Managers:** Ensure that their teams complete the required cybersecurity training and reinforce the importance of cybersecurity best practices.
- **Employees:** All employees are responsible for completing the assigned training and applying the principles learned to their daily work activities.

25-002.7 Compliance and Monitoring: The organization will track the completion of all cybersecurity training. Employees who fail to complete the required training within the specified time frame may face disciplinary action, up to and including termination.

25-002.8 Review and Update: This policy will be reviewed annually and updated as necessary to reflect changes in cybersecurity threats, technology, or legal requirements.

THE FOREGOING was adopted by vote of the Board of Directors of the California Electronic Recording Transaction Network Authority (CeRTNA) this 9th day of April 2025.

AYES:
NOES:
ABSTAIN:

BY:_____
Sheri Thomas, Chairman, Board of Director

* * * * *

STATE OF CALIFORNIA)
) ss.
COUNTY OF INYO)

I, Caroline Nott, Secretary to the California Electronic Recording Transaction Network Authority (CeRTNA), hereby certify the foregoing to be a full, true and correct copy of the record of the action taken by the Board of Directors, by vote of the members present, as the same appears in the Official Minutes of said Board at its meeting of April 09, 2025.

ATTEST:

_____
Caroline Nott, Secretary
Board of Directors