Greater Albuquerque Association of REALTORS® Cybersecurity Policy

1. Purpose & Scope

This policy establishes cybersecurity guidelines for the Greater Albuquerque Association of REALTORS® (GAAR) members, employees, contractors, and third-party vendors who have access—whether temporary or permanent—to GAAR's information systems and data (collectively, "Users"). It applies to all digital assets, including hardware, software, networks, and any data stored, processed, or transmitted.

2. Confidential Data Protection

Confidential data is information whose unauthorized use, access, disclosure, modification, or loss could result in financial, operational, or reputational harm to GAAR, its employees, members, and affiliates. Confidential data includes, but is not limited to:

- Unpublished financial information
- Member records, personnel files, and sensitive business data
- Vendor and partner information
- Credit card and payment details

Data security is the responsibility of all Users.

3. Securing Personal & Company Devices

GAAR contracts with Steady Networks for all IT management for its employees. If you are experiencing a problem, contact GAAR CEO or GAAR Staff for any technical assistance. All individuals accessing GAAR systems must adhere to the following security measures:

- Regularly update software, operating systems, and antivirus programs to prevent vulnerabilities.
- Use strong, unique passwords for all accounts and devices; passwords must not be shared.
- Enable encryption to secure stored and transmitted data.
- Avoid opening suspicious emails or links; report phishing attempts to GAAR IT.
- Install only GAAR-approved antivirus software—third-party antivirus programs are prohibited unless sanctioned by GAAR IT.
- Enable firewalls and secure network configurations to defend against cyber threats.

- Activate two-factor authentication (2FA) for enhanced security.
- Regularly back up critical data to secure storage locations to ensure recovery in case of a breach or device failure.
- Report lost or stolen devices immediately to GAAR CEO and GAAR IT for rapid risk mitigation.

4. Email Security Best Practices

To mitigate risks associated with email-based cyber threats, all employees and members must:

- Verify sender credentials before responding to requests for sensitive data.
- Avoid clicking unknown links or downloading unsolicited attachments.
- Be cautious of clickbait titles and fraudulent messages.
- Look for phishing indicators like poor grammar, excessive capitalization, or unusual urgency.
- Enable email filtering to reduce exposure to harmful messages.

5. Password Management Guidelines

Password security is critical in preventing unauthorized system access. GAAR requires the following standards:

- Use a combination of uppercase and lowercase letters, numbers, and special characters.
- Ensure passwords are at least 12 characters long.
- Never reuse passwords across multiple accounts.
- Enable a GAAR-approved password manager to securely store credentials.
- Change passwords periodically and immediately after a security incident.
- Enable multi-factor authentication (MFA) on all critical systems.

6. Data Transfer Security

To prevent unauthorized access or leaks when transferring sensitive data, individuals must:

- Limit sharing confidential information unless absolutely necessary.
- Use GAAR's official network or encrypted systems for data transfers.
- Ensure data recipients have verified security protocols.
- Report any suspected data breaches immediately to GAAR CEO.

7.Cybersecurity Insurance & Protection

GAAR leadership will annually review cybersecurity insurance coverage provided through the National Association of REALTORS® (NAR), ensuring optimal protection against cyber threats. Additional safeguards will be evaluated as well.

8.Cybersecurity Tips

GAAR encourages the following cybersecurity best practices:

- Never click unknown attachments or links, they may install malware.
- Use encrypted email platforms for sharing sensitive information.
- Secure all login credentials and access codes.
- Periodically purge and archive emails securely.
- Use long, complex passwords and enable two-factor authentication.
- Avoid conducting business over unsecured Wi-Fi.
- Keep antivirus programs, firewalls, and software up to date.
- Back up essential data to separate, secure locations.
- Verify legitimacy before downloading any new apps.
- Report suspicious activity immediately to GAAR staff or leadership.

9. Compliance with Law

Users must comply with applicable federal, state, and contractual obligations relating to cybersecurity and privacy.