Cybersecurity Policy

Effective 5/1/2026

The Real Estate Industry is heavily targeted by cybersecurity threats. Inman News reported over $969M stolen from buyers in 2018 due to cyber crime, and we've seen a ramp up of sophisticated cyber threats come in to both employees and agents in the past year. With AI, we can only expect the level of sophistication to increase.

---

1. Purpose

This Cybersecurity Policy establishes the standards and procedures required to protect the confidentiality, integrity, and availability of company data, systems, and client information. As a real estate brokerage handling sensitive financial and personal data, safeguarding against cyber threats is essential to maintaining trust, legal compliance, and operational continuity.

---

2. Scope

This policy applies to:

- All employees, licensed agents, and contractors
- All devices used for business purposes (company-owned or personal)
- All systems, networks, applications, and data associated with the brokerage

---

3. Data Protection & Privacy

3.1 Sensitive Information

Employees and agents must protect:

- Client personal identifiable information (PII)

- Financial and transaction records
- Contracts, legal documents, and closing details

3.2 Data Handling

- Access sensitive data only when necessary for business purposes
- Store documents in secure, multi-factor authenticated systems such as ZipFormPlus and Google Drive
- Secure personal devices with a password and/or two-factor authentication (facial recognition, biometric identification)
- It is recommended to NOT store documents on your computer. Instead, use an encrypted Transaction Management program to store contracts and other sensitive documents (eg. Zipmforms).

---

4. Password & Authentication Requirements

- Use strong passwords (minimum 8 characters, mix of letters, numbers, symbols)
- Do not reuse passwords across systems
- Enable multi-factor authentication (MFA) wherever available
- Never share login credentials
- Use an approved password manager if needed
- Move toward passwords with 12 characters:

8 vs 12 Characters (Real Difference)

- **8-character password**
  - Possible combinations: ~6.6 quadrillion (6.6×10^{15})
  - Modern cracking tools can guess this in **minutes to hours** if hashes are weak or exposed
- **12-character password**
  - Possible combinations: ~95 quintillion (9.5×10^{22})
  - Would take **thousands of years** to crack with current technology (assuming no shortcuts)

---

5. Email & Phishing Security

- NEVER change bank information or send money to a new client, vendor, agent or employee without calling a KNOWN phone number to verify the information over the phone or speaking with them in person

- NEVER accept a Zoom or other communication link. Always either initiate the zoom link or communicate another way.
- NEVER move the conversation to What'sApp

- Verify all email requests involving financial transactions or sensitive data in person or over the phone via a known method of communication
- Be cautious of unexpected attachments or links.
- Look carefully at the email address of the sender when you receive a suspicious email
- Report phishing emails through the email provider
- Confirm ACH/wire transfer instructions via a secondary communication method (e.g., phone call)
- On social media, it's preferable to use a lead form that advertising your email address, or use a public facing email with a private one for transaction-based emails.

---

6. Device Security

6.1 Approved Devices

- Use only devices with passwords and/or two-factor authentication for business operations
- Keep operating systems and software updated
- Do not log client devices into the company WiFi

6.2 Mobile Devices

- Enable device lock (PIN, biometric, or password)
- Enable automatic screen locking after a period of inactivity
- Report lost or stolen devices immediately, and change passwords to business-related applications
- Applications from untrusted sources or those requesting excessive permissions should be avoided
- Devices that are "jailbroken" or "rooted," or otherwise modified to bypass built-in security controls, are prohibited from accessing company systems.
- Maintain current operating system and security updates
- Use up-to-date antivirus/anti-malware protection where applicable

---

7. Network Security

- Use secure, password-protected Wi-Fi networks
- Avoid conducting business over public Wi-Fi unless using a VPN or password-protected personal hotspot
- Do not connect unauthorized devices to company networks

---

8. Remote Work Guidelines

- Access company systems only through secure connections
- Ensure physical security of devices when working remotely
- Do not leave sensitive information visible in public or shared spaces
- Avoid conducting business over public Wi-Fi unless using a VPN

---

9. Software & Systems Use

- Regularly update all applications to patch security vulnerabilities

---

10. Fraud/Incident Reporting

Employees and agents must immediately report:

- Suspected data breaches - so we can contact IT if necessary
- Phishing attempts - so we can warn others
- Lost or stolen devices - so we can re-sent passwords for company applications
- Unauthorized system access that could be problematic

- If your client is a victim of cyber or wire fraud, immediately alert the Broker and other interested parties to let them know their email may have been compromised
- In cases where fraud is suspected, change user names and passwords, assume you've been compromised and act accordingly to clean your computer and report any possible network breaches.
- Fraud can be reported to the FBI via their Internet Crime Complaint center: https://www.ic3.gov/

---

11. Training & Awareness

- All agents must complete cybersecurity training through Continuing Education training
- Ongoing awareness communications will be provided
- Employees are responsible for staying informed about emerging threats

---

12. Client Protection

- Go over the Wire Fraud form with clients and include a signed copy with brokerage file documents. Agents and brokers in Texas HAVE been fined for defrauded clients when this form is not present.
- Remind clients to never send wires without first calling a known phone number (not one in the email) to verify
- If fraud is suspected, immediately contact Ryan Newlin to report the incident. Our brokerage does carry Cyber Insurance in addition to E&O Insurance.
- Have them turn their social media posts about moving/selling/buying to private, at least until after close.
- Set up Google Alerts on every buyer, seller and listing address. A **Google Alert** is a free monitoring tool from Google that automatically notifies you when new content appears online matching specific keywords you choose.
- Warn your clients against clicking on things they don't recognize and not taking "what is my pet's name" surveys.
- Warn them about scams after closing

End of Policy