Metro South Association of REALTORS®
Cybersecurity Policy – BOD Approved 11/20/2025

Cybersecurity Policy

This policy applies to all members, employees, contractors, and third-party vendors who have access, even temporarily, to MSAR's information systems and data. It covers all digital assets including hardware, software, networks, and data stored or transmitted in any form.

Confidential Data

Confidential data is information for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the organization, employees, affiliates, or members. Confidential data includes, but is not limited to:

- Unpublished financial information
- Data of members, partners, and vendors
- Member records and personnel files
- Credit Card Numbers

Data security is the responsibility of all employees.

Securing Personal and Company Devices

- Regularly update operating systems, applications, and antivirus software to patch vulnerabilities and defend against cyber-attacks or threats.
- Set strong, unique passwords for all accounts and devices. Avoid using easily guessable passwords or sharing them with others.
- Activate encryption features on devices to safeguard data in case of theft or unauthorized access. Encrypt hard drives or utilize built-in encryption tools.
- Exercise caution when opening emails from unknown senders or clicking on suspicious links. Report phishing attempts to the IT department immediately.
- Only install company-endorsed antivirus software on personal and company devices to detect and remove malware, ransomware, and other malicious software. Do not download antivirus software that hasn't been approved by the association.
- Enable firewalls on devices to monitor and control incoming and outgoing network traffic, providing an additional layer of defense against cyber threats.
- Connect to secure Wi-Fi networks and avoid using public or unsecured networks whenever possible. Use virtual private networks (VPNs) for added security when accessing company resources remotely.
- Implement two-factor authentication (2FA) on accounts and devices to add an extra layer of security beyond passwords. This helps prevent unauthorized access even if passwords are compromised.
- Regularly back up important data regularly to external drives or secure cloud storage services. In the event of device loss or data corruption, backups ensure data recovery.

- Immediately report lost or stolen personal or association devices to the Association Executive or President to initiate remote wiping procedures and prevent unauthorized access to sensitive information.

Email Security

- Be cautious of emails requesting sensitive information, urging immediate action, or using urgent language. Verify the sender's email address and scrutinize unexpected requests for personal data or financial information.
- Exercise caution when clicking on links or downloading attachments from unknown or unexpected sources or when the content is not adequately explained. Hover over links to verify the URL's legitimacy, and only open attachments from trusted senders. When in doubt, verify with the sender through a separate communication channel.
- Be suspicious of clickbait titles (e.g. offering prices, advice)
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).
- Enable spam filters and email filtering mechanisms provided by your email service provider to automatically identify and divert suspicious or malicious emails to the spam or junk folder. Regularly review the spam folder to ensure legitimate emails are not mistakenly flagged.

Password Management

- Use a combination of uppercase and lowercase letters, numbers, and special characters (!, @, #, $, etc.) to increase the complexity of your password.
- Aim for a minimum password length of 12 characters or more to make it harder for attackers to crack.
- Use a long, nonsensical phrase (not song lyrics or famous quotes), with each word separated by a space.
- Avoid using dictionary words or common phrases, as these are easily guessable by attackers using automated tools.
- Generate random passwords using a mix of characters to enhance security. Avoid using easily guessable patterns or sequences.
- Ensure each password is unique and not reused across multiple accounts. This prevents a single compromised password from compromising multiple accounts.
- While regular password changes were once recommended, recent guidelines suggest focusing more on creating strong, unique passwords rather than frequent changes. However, it's still good practice to change passwords periodically, such as every three to six months, especially for critical accounts or in response to security incidents.
- The association utilizes the services of a password management tool which generates and stores passwords. Employees are obligated to create a secure password for the tool itself, following the abovementioned advice.

- Choose a strong, memorable master password to access your password manager. Avoid using easily guessable information, such as birthdays or common phrases.
- Enable multi-factor authentication, where available, for an extra layer of security. This typically involves verifying your identity using a second factor, such as a code sent to your mobile device.
- Regularly back up your password manager's vault and enable synchronization across your devices to ensure access to your passwords from anywhere while maintaining security.

Data Transfer Security

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless necessary.
- Share confidential data over the company network/system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts to the Association Executive or President.

Insurance

Annually review the Association's cybersecurity insurance coverage provided by the National Association of REALTORS® and the availability and applicability of products such as social engineering fraud endorsements and computer and electronic crime riders.

Cybersecurity Tips

- Never click on unknown attachments or links, as doing so can download malware onto your device.
- Use encrypted email, a transaction management platform, or a document-sharing program to share sensitive information.
- Carefully guard login and access credentials to email and other services used in the transaction.
- Regularly purge your email account and archive important emails in a secure location.
- Use long, complicated passwords such as phrases or a combination of letters, numbers, symbols.
- Do not use the same password for multiple accounts.
- Use a password manager.
- Use two-factor authentication whenever it is available.
- Avoid doing business over public, unsecured Wi-Fi.
- Keep antivirus software and firewalls active and up to date.
- Keep your operating system and programs patched and up to date.

- Regularly back up critical data, applications, and systems, and keep backed up data separate from online systems.
- Don’t download apps without verifying that they are legitimate and won’t install malware or breach privacy.
- Don’t click on links in emails and texts from unknown senders.