**CP-30 Commission Position on Data Security and Privacy**

Adopted October 1, 2024

---

Real estate transactions involve the exchange of sensitive information. Sensitive information is information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the owner of the information, leading to identity theft, financial loss, and other harms. Sensitive information includes personally identifiable information (PII) that is critical to an individual's privacy, financial security and legal compliance. The exchange of such information by digital methods leads to an increased risk to Brokers and their clients of a data breach. Brokers have an on-going obligation to preserve the confidentiality of all sensitive data and information provided to them by Clients, or on the clients' behalf; this duty continues even after the termination of the brokerage relationship. This obligation exists for all Brokers, whether acting in the capacity of a Transaction-Broker or pursuant to an Agency agreement. License law contemplates the requirement for brokers to comply with local, state and federal laws and regulations, including, but not limited to: Commission Rule 6.4.C., Policy on the Destruction or Disposal of Personal Identifying Information and § 6-1-716, C.R.S. It is also imperative for Brokers to be alert to potential cybersecurity risks and take proactive measures to protect a client's sensitive or confidential information. Some examples of cybersecurity best practices are provided below and are not an exhaustive list.

**Conduct a Cybersecurity Threat Assessment:** It is recommended that Brokers conduct an inventory of all sensitive information that their business uses. This assessment should evaluate how the information is obtained, how it is received and stored, and who has access to it. This includes identifying the computers and servers where sensitive information is stored, and all means of accessing such information. An assessment should be made of the vulnerability of these systems to commonly known threats.

**Email Accounts:** Brokers should avoid using a free web-based email service account and should consider using a propriety email account instead. Brokers can also advise Clients about the risk to THEIR free web-based emails. Many times, it is the Client's email that was compromised, leading to a security breach. Brokers should use a regulated email server with firewall and anti-virus protection. It is also recommended that Brokers use encryption software to protect the transmission of financial or other personal information. Brokers should periodically review the security and privacy settings for their email accounts. This can include checking sent emails for responses that the Broker did not send and regularly check email "rules" to ensure nothing has been created without the Broker's knowledge.

**Email Use Best Practices:** Brokers should avoid using their personal email accounts for any professional emails or a professional account for personal emails. Always log out of your email account when finished. Brokers should never ask for or provide sensitive information in an unsecured email. Brokers should use caution in opening emails from unknown senders and should be particularly cautious of opening attachments or clicking on links in such emails. Some things to consider in evaluating emails that appear suspicious are whether it contains typos, unusual URLs, or requests for personal information, demands an urgent response, or comes from an email address that does not match the company's name.

**Passwords:** Simple and short passwords should not be used; experts suggest using at least 12 characters and ideally 16 or more. For example, a strong password could include a phrase password with numbers and special characters or a string of words that are unrelated (e.g.: horsehousehallwayhappy). The same password should not be used on more than one system; one example of this is that a password used for any work platforms should not also be used on social media accounts. Passwords should be frequently updated. Consider using a password manager to help track and store all passwords securely.

**Protect Networks and Devices:** Wi-Fi networks should be secured with strong encryption, unique passwords, and regular monitoring to prevent unauthorized access. A Wi-Fi router's firmware and software should be regularly updated to ensure it has the latest security enhancements and patches. Devices should have antivirus, anti-spyware, encryption, and anti-malware software installed and regularly receive software updates. If sensitive information is not encrypted, anonymized, or otherwise secured, information on lost or stolen devices can be compromised. Brokers should consider using a firewall to protect their systems.

**Public Wi-Fi:** Using an unsecured public Wi-Fi can leave someone vulnerable to cybercrime. Virtual private networks (VPNs) encrypt internet connections, making it much harder for cybercriminals to intercept and steal data. Consider setting up a VPN on your devices for an extra layer of security when accessing sensitive information over public Wi-Fi networks. VPNS are also beneficial for individuals working remotely, as unsecured home Wi-Fi networks can also expose sensitive data to potential threats.

**Multi-Factor Authentication:** Multi-factor authentication (MFA) should be used for all networks to verify the identity of a user before they are allowed access to sensitive information. MFA requires at least two forms of identification for added protection such as passwords and security tokens, through a cell phone app or text, as well as biometric options such as facial recognition or fingerprint scans. When MFA is enabled, even if a hacker has access to a password, the account cannot be accessed without an additional authentication. This effectively eliminates phishing as a problem for accounts where it is enabled.

**Document Sharing Platforms:** It is recommended that Brokers utilize secure document-sharing platforms that allow users to share sensitive information while maintaining confidentiality and security. These platforms utilize access controls, encryption, and other security measures to protect documents from unauthorized access or data breaches.

**Wire Transfers:** Brokers should advise clients to provide wiring instructions to the title company, in person, at closing. If a Broker will be providing wiring instructions to the title company on behalf of their client, those instructions should be provided to the title company in person, at closing. It is advised that no wire transfer is made based only on an email. However, if it is not possible to provide wiring instructions in person at closing and the title company is willing to accept wiring instructions in a different format (e.g. U.S. mail), wiring instructions should be verified over the phone with the title company. When verifying wiring instructions by phone, only use a phone number that was previously verified; not a phone number found in an email.

**Third-Party Vendors:** When engaging third-party vendors to whom you are providing sensitive information, thoroughly review their privacy policies carefully to ensure that these vendors meet your security standards and practices and reach a clear agreement on security expectations and response protocols.

**Provide Cybersecurity Training and Education for Brokers:** Regularly providing individuals under your supervision with up-to-date information regarding the latest cybersecurity risks and cybersecurity best practices allows them to take the necessary steps to protect both themselves and their clients.