Last Updated: February 1, 2021

8. LICENSEE OBLIGATIONS FOR SECURITY OF CONFIDENTIAL INFORMATION

Purpose

This document sets out the HCRA's expectations of licensees to manage and protect the confidentiality of personal and commercially sensitive information a licensee collects, uses, or shares while operating as a builder and/or vendor.

Obligation

All licensees have a legal obligation to manage and protect confidential information as part of their operations. This includes information included in digital and paper-based formats. Under the New Home Construction Licensing Act, 2017, the General Regulation, O. Reg 626/20, section 3 paragraph 1 states:

A licensee shall maintain reasonable data security measures to protect the personal and other information it collects, retains, uses, transfers, discloses and disposes of.

Scope of Confidential Information

In the course of its operations, a licensee may receive or create information that should be kept confidential and private. This personal and commercially sensitive information includes information that should only be released to specific individuals or entities for specific purposes. This includes information in digital and paper-based formats. This information is collectively referred to as "confidential information".

HCRA Guidelines for Protecting Confidential Information

1. Confidentiality

The HCRA expects licensees to create a confidentiality policy to protect confidential information. A written and signed confidentiality agreement must be in place between all licensees and their staff, agents, and/or independent contractors to clearly communicate and acknowledge their responsibilities for how they obtain, store, access, and dispose of confidential information in respect of consumers, employees, and commercial operations of the licensee.

2. Keeping Confidential Information Secure

It is important to ensure that all confidential information remains secure, particularly when it is being distributed. This means only those who are entitled and authorized to handle confidential information should have access and permission to share this information. Licensees are required to have a policy on how they keep information secure. There are several ways to ensure information remains secure:

a. Sending and Receiving Information

When individuals need to send confidential information outside of the licensee's offices, steps need to be taken to ensure the information is secure and cannot be viewed by persons other than the intended recipient.

Electronic copies of confidential information must be transported in an encrypted form, that is not easily accessible, such as through a password protected device or cloud service. Emailing confidential files to personal email accounts, such as Hotmail and Gmail is not advised because once an email has been sent, the security of the information cannot be controlled. The use of email to transmit confidential information is not recommended unless both parties agree to keep the material confidential.

Paper copies of confidential information must be transported with care. Files and documents should never be left unattended where the information can be viewed by others.

b. Sharing Information

The HCRA reminds licensees that online or social media platforms like Twitter, Facebook, Instagram, chat rooms, wikis, or blogs are public. Those who wish to use social media platforms must not discuss or share confidential information in any public forum.

Individuals must also be cautious when discussing confidential information with individuals outside of work. For instance, individuals must take efforts to ensure that confidential information is not discussed in open public settings, where it may be overheard by others.

c. Storing Information

Information must be stored in a secure manner. Hard copies of files or documents must be stored in a secure place only accessible to those who have authorization to handle confidential information. Electronic copies must be stored on devices that have security features, including password protected access and/or hard drive encryption. If cloud storage platforms are used, the licensee should confirm that security features prevent external unauthorized access to confidential information.
The expectation is that confidential information will not be stored permanently, instead it will only be stored for the duration required to complete the task or project at hand, or for the duration of the warranty, or for any legal reason to keep that information for a longer period (e.g. potential legal cases).

d. Destroying Information

The HCRA expects licensees to destroy all confidential information in a secure manner, which is part of their policy on protecting confidential information.

Electronic files of confidential information must be permanently deleted from each location where they have been saved. For example, internal and external hard drives, USB drives, network drives, and smartphones and other mobile devices. If applicable, delete the information from the 'deleted items' or 'trash folder.' Paper copies of confidential information must be securely shredded.

3. Information Breach

Complying with the expectations articulated in this document will help to ensure confidentiality of information is protected. There may be situations where, despite these practices, concerns are raised that confidentiality of information has been compromised and an information breach may have occurred. The licensee must inform the HCRA of a significant breach of confidentiality.

Licensees, their employees, and contractors are required to uphold the licensee's policy on information security. Should a licensee's employee or contractor suspect that a breach has occurred, the licensee must be informed immediately. The HCRA expects that licensees will carefully assess the situation and take any necessary steps to minimize the exposure of information, such as contacting the police, any individual or business whose information may have been compromised, and anyone else who should reasonably be informed of the breach.

Failure to Keep Information Secure

The licensee is required, as a condition of their license, to protect the confidential information they obtain. Failure to implement reasonable measures to protect the security of confidential information is contrary to the condition of licence in the Regulations and could result in licensing compliance actions, such as additional conditions on a licence, education or training requirements, or other actions as appropriate in the circumstances.

Resources

Licensees who engage in commercial activities must also comply with the *Personal Information Protection and Electronic Documents Act* (Canada). For more information, please see the Privacy Commissioner of Canada's guide to the Act for businesses: https://www.priv.gc.ca/media/2038/guide_org_e.pdf