

# Internet Security

## Internet Security Statement

GWL Realty Advisors Residential (“**GWLRA Residential**”) recognizes and respects the importance of security. This Internet Security Statement covers the measures that GWLRA Residential takes to help secure your personal information. This Internet Security Statement is subject to change without notice to you, so we recommend that you review it regularly. By using this site, you acknowledge that you have read and understood this Internet Security Statement as amended from time to time.

## Encryption

Encryption technology is designed to secure personal and confidential communications between your computer and GWLRA Residential servers, such that they are protected from being read by any third parties. This is achieved by “scrambling” communications so that they are unreadable by anyone other than GWLRA Residential or yourself. GWLRA Residential web applications provide a minimum of 128-bit encryption. You can verify that a GWLRA Residential website is encrypted by looking for the golden lock or key icon along the bottom of your browser window, which is used by most browsers to indicate a secure connection.

## Cookies

“Cookies” are small items of data that websites store in your browser. These data files contain information the site can use to track and organize the pages you have visited, and to gather information. Some GWLRA Residential websites use “cookie” technology to measure site activity and tailor information to fit your personal interests. This helps us deliver a superior website experience that is fast, secure and personalized.

## Timeouts and Automatic Logouts

Some GWLRA Residential websites may require you to log in using a username and password. While you are logged in, if you leave your browser window open, GWLRA Residential applications may automatically log you out after a period of inactivity. Similarly, if you close your browser window without logging out, you may be automatically logged out. Both of these measures are designed to protect your information from unintended access by a passerby or different user of your computer.

## Fraud

Be cautious of email and websites purporting to represent a legitimate company and that ask you to provide confidential or financial information. This is called *phishing*. The content of a phishing email or text message is intended to trigger a quick reaction from you. It can use upsetting or exciting information, demand an urgent response or employ a false pretense or statement. Phishing messages are normally not personalized.

It is not GWLRA Residential's practice to email you to ask you to provide or confirm your PIN, password, or other confidential or financial information, other than as may occur in response to an inquiry from you.

If you receive such a request, or if you have any concern as to the validity of an email from GWLRA Residential, a website claiming to be a GWLRA Residential website, a digital communication claiming to be from GWLRA Residential and its employees or our online security, please contact our Special Investigations Unit toll free at 1-877-751-4317 or [email us](#).

Please attach any suspicious email in its original form, or in the case of a website, please include the URL (address of the website) in your notification.

For information on various types of email fraud and phishing, please visit the [email fraud / phishing](#) page on the RCMP website.

## Other Security Measures

GWLRA Residential engages in a number of other security activities to help ensure the safety and privacy of your personal information. This includes adopting measures to help secure our computers against hacker attacks and virus activities by a number of different means. We monitor our website, servers, email, and data 24 hours a day to help us immediately identify and rectify any problems. Note that all

emails and attachments sent to the organization may be scanned for viruses by a third-party service provider. Scanning may take place outside of Canada.

## Security Tips You Can Use

You can also contribute to the security of your information by following a few straightforward principles:

For GWLRA Residential sites requiring a password:

- Pick a password that is unique and hard for others to guess. A strong password includes a combination of upper- and lower-case letters and numbers. Avoid passwords such as family or pet names, birthdays, or words found in dictionaries.
- Memorize your password, and don't tell it to anyone. Remember that no one from GWLRA Residential will ever call or email asking for your password.
- If you think anyone has had access to your password, change it immediately by logging in and clicking the Your Profile tab. From the Your Profile section, follow the simple instructions to change your password.
- If you are using a computer in a public place (such as an Internet café, or an open desk at work), ensure that no one can see you type in your password, log off when you are finished using the site and clear the browser's cache.
- Run current anti-virus software and anti-spyware software on your computer. This helps ensure your computer is free of malicious programs such as viruses, worms and spyware (snooping software that collects and shares confidential information on your computer with a third party without your consent).
- After using a GWLRA Residential application, clear your browser's cache and then close it. The cache is where a browser keeps copies of the web pages you have recently visited. By clearing it, you help ensure no one else can view these pages, including the next website you visit.