Security Policy

LAWPRO's Security Policy outlines the measures and procedures undertaken by LAWPRO to ensure that the personal information of our customers and employees is kept private and secure, in accordance with the terms of our Privacy Code. Therefore, this Security Policy complements LAWPRO 's Privacy Code, available at www.lawpro.ca/privacy.

In this Policy, "we", "us" and "our" means Lawyers' Professional Indemnity Company (LAWPRO), which includes TitlePLUS® and practicePRO®. "You" and "your" means the individual who is a customer or potential customer of LAWPRO.

Our websites may contain links to other websites that are provided and maintained exclusively by third parties. Websites provided and maintained by third parties are not subject to this Security Policy. Please review the security policies on those websites to determine their practices.

Internal Security Controls

Only certain LAWPRO staff who, because of the nature of their work, must have access to information about you can retrieve information from your master record. In other words, specific system, database, or application access is granted on an "as needed" basis and controlled on the basis of job function. Such access is audited on an annual basis.

Unique user IDs and passwords are required for access to all LAWPRO computer systems; staff users are responsible, and held accountable, for the assigned ID. Passwords are not to be shared among users and are changed on a regular basis.

When one of our staff users has a significant change in duties, such as a transfer to another department, the user's access permissions are reviewed and modified. If the user's new department and responsibilities no longer require access to certain information, that access is removed. User accounts are disabled upon termination of employment or contract.

LAWPRO's computer systems also have built-in audit functions that track access and modification of data. These audit logs can be used to identify and track unauthorised attempts to access information.

Storage of personal information is not permitted on a routine basis on our desktop or laptop computer hard drives. All computer files containing personal information are centralised on our secure servers, which are backed up on a nightly basis. Direct access to core databases is not permitted. Special software applications are used to control access and maintain the security and accuracy of the data in the systems.

Staff are aware that personal information (including data stored in paper files or documents, or digital media like tapes, CDs/DVDs or USB drives) must not be left out in plain view where any unauthorised viewing or access by outsiders could occur. Our staff must log out of all applications and shut down their desktop computers at the end of each day, and are required to

close down applications containing personal information when absent from their desks for extended periods of time.

Access to paper files is controlled by a sign-in/sign-out procedure. LAWPRO employs a secure document disposal and shredding service to ensure the security of discarded paper documents and files.

External Access Controls

To protect the security and privacy of your personal information from unauthorised external access, access to LAWPRO's premises are controlled by reception staff and security card inspection. Remote access to LAWPRO computer systems by staff is limited by user IDs and passwords, and is permitted on an "as needed" basis.

Entry to LAWPRO websites is protected by firewall and routing software, and by access controls installed on the website servers. Critical servers are monitored by intrusion detection software, which reports unauthorised access or changes to the system. LAWPRO's security procedures are also audited by two external firms for security compliance and adherence to best practices.

Network and Server Security

LAWPRO's network and servers are protected in limited access, climate-controlled facilities. Access to LAWPRO equipment is only authorized for designated members of LAWPRO's Information Systems Department and vendor technicians explicitly authorized by LAWPRO personnel. Such technicians are supervised by LAWPRO personnel and/or bound by the terms of a confidentiality agreement.

The stability of the systems is assured by redundant backup power supplies and redundant "fail-over" hardware components built into the servers. Firewall rules are updated regularly, Virus definitions are updated multiple times each day, and virus scanning and web filtering software operates throughout the network and on all desktop computers and laptops.

Data transmitted within LAWPRO on its private network (or intranet) is not encrypted, nor are routine e-mail communications leaving the LAWPRO network. However, staff are encouraged to consider the sensitivity of material before transmitting it outside the network by e-mail.

Nightly backups are performed on all systems, with backup tapes being stored securely off-site for disaster recovery purposes. Only authorized LAWPRO personnel and employees of the off-site tape management facility have access to the backup data.

Disaster recovery tests are performed regularly.

Web Security

1. Our Visitors: What we know

When you visit the informational (or non-secure) areas of our websites, only the following information is tracked:

- the name of the domain from which you access the Internet (for example, "sympatico.ca" or "aol.com");
- the date and time you access our sites;

the pages and files that were accessed on the site; and

the Internet address of the website from which you linked to our site (for example, from the "Links" page on a different site).

Except as noted below, this information is only stored/reviewed in aggregate form, and only in order to monitor traffic patterns and volumes of use. We do not look at an individual's use of our websites.

However, LAWPRO does use industry-standard methods to identify unauthorised attempts to access, change or disrupt our websites or data. Such unauthorised access is strictly prohibited, and may be reported to the appropriate authorities and Internet service providers.

2. SSL and Encryption

In order to help protect your security when you communicate with LAWPRO through our family of websites, we recommend that you use a web browser that supports 128-bit encryption - a strong, relatively secure form of encryption that is generally viewed as providing adequate protection when transmitting confidential data over the Internet. .

As a general rule, to make sure that you have established an SSL (Secure Socket Layer) connection, confirm that the website address is displayed with "https://", rather than the standard "http://". More information about your preferred browser and how it supports SSL connections and encryption is available online. For Internet Explorer, visit www.microsoft.com/ie; for Firefox, visit mozilla.com/firefox; for Chrome, visit google.com/chrome; for Safari, visit apple.com/safari.

If you do not have a browser that supports encryption, contact your computer system administrator for advice.

3. Logging In

For your protection, we require that you "log in" to secure areas of our websites using your lawyer member number (or firm number) and a password that you have selected. We suggest that you use a combination of letters and words for your password. Do not use words that can be associated with you easily, and change your password regularly.

Your password should be kept secret at all times because it is used to help verify your identity before you are permitted access to certain confidential information, such as your insurance policy and address information. If you are unable to provide the correct password, you will not be granted access. Invalid password attempts are tracked by the system; for security purposes, an account will be “locked out” in the event of several consecutive invalid password attempts.

LAWPRO recommends that shared computers have browsers set to NOT save passwords for future use. This option is available in all modern web browsers. We provide a number of convenient options for being reminded of your password, when necessary, including an online reminder/validation or a call-back service from our Customer Service Department.

When you log in successfully, your web browser will establish a secure SSL connection between your computer and our website. When you leave the secure portion of our website, you will get a notification from your web browser that you are leaving the secure section, and returning to an open section.

4. Timed Logout
To further protect against unauthorised access to your accounts, our systems are designed to automatically log out if a secure online session is inactive for more than one hour. If your session terminates, you will be prompted for your lawyer/firm number and password again before you can resume your online activities. Since most transactions on LAWPRO's family of websites take only minutes, this should rarely pose a problem.

5. Cache Storage
The "cache" storage in an Internet browser consists of copies of pages you have visited and information that you have entered during the course of your browsing session. Your browser also relies on its cached web pages when you use the "Back" button on your browser.

For your transactions with LAWPRO's websites to work properly, caching must be activated on your web browser before using the site. However, to protect the confidentiality of your personal information, you may choose to clear your browser's memory cache after completing your browsing session.

More information about managing and clearing the cache from your preferred browser is available online. For Internet Explorer, visit www.microsoft.com/ie; for Firefox, visit mozilla.com/firefox; for Chrome, visit google.com/chrome; for Safari, visit apple.com/safari.

6. Cookies
In order for our websites to confirm and re-confirm your identity throughout the course of your transactions and e-filing, we make use of "cookies," which are small text files sent by a website to your Internet browser and stored on your computer. There are two types of cookies: "session" cookies and "persistent" cookies. The primary difference between session cookies and persistent cookies is that session cookies expire when you have finished your browsing session (e.g., you have closed your browser, or left it idle for an extended period of time), while persistent cookies may remain on your computer even after you have completed your browsing.

It is important to remember the following facts about cookies:

- they can only be read by the website that placed them;
- they cannot be used to track visits to other websites;
- they cannot run malicious code or viruses; and
- they cannot search outside your browser into your computer for information or download data.

Like most e-commerce facilities, LAWPRO's family of websites makes use of cookies in order to provide a more convenient and secure transaction over the Internet. LAWPRO's websites only use session cookies, and do not use persistent cookies. For your security, in order to use the secure section of LAWPRO's websites, you must have session cookies enabled.

More information about your preferred browser and how it supports cookies is available online. For Internet Explorer, visit www.microsoft.com/ie; for Firefox, visit mozilla.com/firefox; for Chrome, visit google.com/chrome; for Safari, visit apple.com/safari.

Destruction Guidelines

LAWPRO recognizes that in order to prevent unauthorized parties from accessing your personal information, it is important to use care in the disposal and destruction of personal information. For the purposes of this section of the Policy, "destruction" (or "destroy") means the taking of steps to ensure that personal information on all storage media (including paper, electronic, audio or video media) cannot later be used or re-constructed, once a decision has been made not to retain specific material.

A destruction record will be maintained by the Chief Information Officer regarding destruction of records in bulk that contain personal information. Any destruction of records in bulk requires the authorization of the Department Head responsible for the records and the Chief Executive Officer (or the delegates of either of them).

In general (and subject to emerging technologies for record destruction), LAWPRO is committed to destroying records using the methods described as follows:

Paper Records:	Shredded or Personal Information redacted.
Electronic:	Under supervision of Information Systems Department, physical destruction of medium or application of appropriate utility to ensure that data cannot be re-constructed.
Video/audio Tapes:	Physical destruction unless overwritten on premises by authorized staff.

Conclusion

Any changes to our Security Policy shall be acknowledged in a timely manner. We may add, modify or remove portions of this Policy when we feel it is appropriate to do so. You may determine when this Policy was last updated by referring to the modification date found on the version of the Policy available at www.lawpro.ca/security

[1] Encryption is a process of scrambling or "encrypting" information for passage across the Internet. For example, information can be scrambled at your computer and then unscrambled (or "decrypted") when it arrives at LAWPRO. This helps prevent the information from being read or intercepted while being transmitted.

[2] Please note that any third party websites referred to in this Policy are not endorsed by LAWPRO and that LAWPRO assumes no responsibility for their contents.

Last updated on June 3, 2013