



LDD[®]'s Security Policy¹

LDD's Security Policy outlines the measures and procedures undertaken by LDD 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 LDD's Privacy Code, available at <http://www.lawyerdonedeal.com/privacy.pdf>.

In this Policy, "we", "us" and "our" means LawyerDoneDeal Corp. ("LDD"), which includes CAKEsoft Inc.. "You" and "your" means the individual who is a customer or potential customer of LDD.

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

Internal Security Controls

Only certain LDD 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.

Unique user IDs and passwords are required for access to all LDD 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. User accounts are disabled and passwords are changed upon termination of employment or contract.

LDD's computer systems also have built-in audit functions that track access. 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, except upon a customer's express instructions, as part of providing work and services, which personal information is deleted from our staff user's computer hard drive once work is completed. All computer files containing personal information are centralised on

¹ This Security Policy also applies to CAKEsoft Inc., a wholly-owned subsidiary of LDD.

our secure servers, which are backed up on a regular basis. Special software applications are used to control access and maintain the security of the data in the systems.

Staff are aware that personal information (including paper files or documents, computer disks, CDs, and tapes) must not be left out in plain view where any unauthorised viewing by outsiders could occur. Our staff must log out of all applications 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.

Paper files are stored in locked cabinets to which only certain LDD staff, due to the nature of their work, have access. Any important documents that are no longer needed and are to be discarded, are shredded in our offices.

External Access Controls

To protect the security and privacy of your personal information from unauthorised external access, access to LDD's premises will be controlled by key-card access as of May 1, 2004. Remote access to LDD computer systems by staff is limited by user IDs and passwords and is permitted on an "as needed" basis.

Entry to LDD Web sites is protected by firewall and routing software, and by access controls installed on the Web site servers. Critical servers are monitored by intrusion detection software, which reports unauthorised access or changes to the system.

Network and Server Security

LDD's network and servers are protected in a limited access server room. Vendor technicians are not permitted in the server room unless an LDD staff-member is in attendance.

The stability of the systems is assured by a UPS (uninterruptible power supply) and where appropriate, hardware redundancy features built into the servers. Industry-standard virus software, updated regularly, is installed on the network and all desktop computers.

Data transmitted within LDD on its private network (or intranet) is not encrypted, nor are routine e-mail communications leaving the LDD network.² However, staff are encouraged to consider the sensitivity of material before transmitting it outside the network by e-mail.

Regular backups are performed on all systems, with backup tapes being stored securely for disaster recovery purposes. Only LDD staff have access to the backup data.

Web Security

1. Our Visitors: What we know

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

² Encryption is a process of scrambling or "encrypting" information for passage across the Internet. For example, information can be scrambled at your PC and then unscrambled (or "decrypted") when it arrives at LDD. This helps prevent the information from being read or intercepted while being transmitted.

- 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 Web site 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 Web sites.

However, LDD does use industry-standard methods to identify unauthorised attempts to access, change or disrupt our Web sites 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 LDD through our family of Web sites, we recommend that you use Netscape Navigator™/Communicator™ or Microsoft® Internet Explorer browsers with 40-bit or 128-bit encryption.

Forty-bit encryption provides basic security and is available in most Internet browsers. For using our Web-based applications, we recommend using a stronger, 128-bit encryption method. Encryption at the 128-bit level is the strongest, most secure form of encryption that is generally available in Internet browsers on the market in North America today.

To check your browser’s encryption level:

For **Netscape Navigator/Communicator, Version 4.x, 6.x, and 7.x**, select Help, About Netscape Navigator/Communicator, and look for the reference to either 40-bit or 128-bit encryption.

During a browsing session, your security level will be shown in one of three ways:

1. If you are on an open section of a Web site, your browser will display an open lock in the bottom left-hand corner of your screen.
2. If you are in a secure portion of a Web site and you have 40-bit encryption, your browser will display a solid key with one tooth in the bottom left-hand corner of your screen.
3. If you are in a secure portion of a Web site and you have 128-bit encryption, your browser will display a solid key with two teeth in the bottom left-hand corner of your screen.

For **Microsoft Internet Explorer 4.x, 5.x, and 6.x**, select Help, About Internet Explorer, and look for the reference to either 40-bit or 128-bit encryption.

During a browsing session, your security level can be checked by selecting the following options from the browser menu bar: File, Properties, Security. By selecting these options, the browser will display details of the security level being used for your current location in the Web site.

To make sure that you have established an SSL (Secure Socket Layer) connection, confirm that the Web site address is displayed with “https://”, rather than the standard “http://”.

If you do not have a browser that supports encryption, contact your computer system administrator for advice. You may also wish to visit Netscape’s Web site (www.netscape.com/download) or Microsoft’s Web site (www.microsoft.com/windows/ie/downloads) for more information and free download instructions.

3. Logging In

For your protection, we require that you “log in” to secure areas of our Web sites using the appropriate user name and password applicable to a particular LDD Web site or application. 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. If you are unable to provide the correct password, you will not be granted access.

We recommend that shared computers have browsers set to NOT save passwords for future use. This option is available in both Internet Explorer and Netscape.

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

4. Timed Logout

For certain applications on our Web sites and 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 LDD’s family of Web sites take only minutes, this should rarely pose a problem. Alternatively and where appropriate, other applications on our Web sites have been designed not to automatically log out to ensure consistency and to reflect user workflow patterns.

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 LDD's Web sites 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. The instructions for clearing cache are as follows:

For **Microsoft Internet Explorer 4.x**, select View, then Internet Options on the menu bar. Click the General tab, then click the Delete Files button. Click OK.

For **Microsoft Internet Explorer 5.x**, select Tools, then Internet Options on the menu bar. Click the General tab, then click the Delete Files button. Click OK.

For **Microsoft Internet Explorer 6.x**, select Tools, then Internet Options on the menu bar. Click the General tab, then click the Delete Files button. Do *not* click the "Delete Cookies" button, unless you wish to clear all cookies from your computer. Click OK.

For **Netscape Navigator/Communicator, Version 4.x**, select Edit, then Preferences on the menu bar. Click Advanced, then Cache. Click the Clear Memory Cache button and the Clear Disk Cache button. Click OK.

6. Cookies

In order for our Web sites to confirm and re-confirm your identity throughout the course of your transactions, we make use of "cookies," which are small text files sent by a Web site 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., 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 Web site that placed them;
- they cannot be used to track visits to other Web sites;
- they cannot run malicious code or viruses; and
- they cannot search outside your browser into your computer for information or download data.

Like most modern Web sites, the LDD family of Web sites makes use of cookies in order to provide a more convenient and secure transaction over the Internet. For your security, in order to use the secure section of LDD's Web sites, you must have session cookies enabled.

For more information about your browser and how it supports cookies, visit:

- For **Netscape Navigator/Communicator, Version 4.x, 6.x, and 7.x**, visit Netscape at http://wp.netscape.com/legal_notices/cookies.html, or
- For **Microsoft Internet Explorer 4.x, 5.x, and 6.x**, visit Microsoft at <http://www.microsoft.com/info/cookies.htm>

Conclusions

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.lawyerdonedeal.com/security.pdf.

® LawyerDoneDeal, LDD and LawyerDoneDeal and Design are registered trademarks of LawyerDoneDeal Corp.
All other trademarks belong to their respective owners.

(revised February 3, 2004)