COMPUTER SECURITY POLICY

It is the policy of *FIRM NAME* (the Firm) to provide computer resources to its professional and administrative staff to assist them in conducting Firm business. Firm business is defined as client-related services that include document generation, electronic communication and electronic research using tools such as the Internet, CD-ROM's, and on-line databases. The Firm does not restrict access to these resources. However the Firm does expect that these resources will be used for business purposes only, and will be billed to clients when appropriate.

The policy of the Firm is further defined below.

Computer Hardware

All hardware owned by the Firm is labeled and recorded in an inventory database. Bar code labels identify equipment by type and location. Generally all Firm-owned computer equipment is on the premises of its various offices, however in some cases equipment is loaned to the professional or administrative staff for business use outside the office.

Loaned Equipment

It is the responsibility of the person who has possession of the equipment to safeguard the equipment against theft or damage. The equipment must be returned to the Firm in the same condition as when it was loaned. This pertains to desktop computers, laptop computers and Blackberry handhelds.

Loaned equipment should not be modified (for example, by adding components such as additional memory, CD-ROM drives, *etc*.) without the express permission of the Firm.

Equipment on Premises

The equipment provided on premises at each of the Firm's offices is the property of the Firm and should be treated as such. Equipment should not be modified without the

express permission of the Firm. Adding peripheral devices such as scanners, speakers, or CD-burners, or otherwise tampering with computer equipment is in violation of the Firm's policies.

Computer Software

The Firm provides the software necessary to conduct the business of the Firm. This software includes but is not limited to a word processor with macros and templates, a spreadsheet program, time entry, email, a calendar, remote access software, and an Internet browser.

Licenses for said software are purchased and maintained by the Firm. Licenses for home use of the software are also provided, and a Software License Agreement must be signed prior to receiving copies of the software. The Software License Agreement stipulates that the software is the property of the Firm and in the event the individual is no longer with the Firm, the software is to be removed from any and all computers on which it was installed, such as home computers, personal palmtops or personal laptops.

Under the Software License Agreement and copyright laws, no individual shall duplicate in any way or distribute software owned by the Firm.

System Security

All Firm work is considered client privileged and confidential. As such, prudent use of the computer systems is warranted to insure security and data integrity. With the increasing reliance on computers, handheld messaging devices, remote access and electronic records, securing the Firm's systems and data are a top priority.

Computer system log on ID's and passwords should not be made public and should be treated in the same way as a bank PIN. Computer system log on passwords should be

changed periodically to maintain security. Users should change the initial access password ("centre") to a unique individual identifier as soon as possible.

No person outside of the Firm should be given access to the Firm's computer system without the express permission of the Firm.

Each person is responsible for logging off the system prior to leaving the office for the day. Logging off during extended absences such as lunch or meetings is encouraged.

System Passwords

Effective May 6, 2003, the Information Technology Department will put into place system settings to enforce the use of "strong" passwords and to force password changes every six months. A strong password is a combination of alpha and numeric characters and is generally considered difficult to crack. Please be prepared to change your password, when prompted, to a password that is a combination of letters and numbers and is six characters in length at a minimum. If you do not comply with the system password requirements (including changing the password every six months), you will **NOT** be able to access the system.

Blackberry Passwords

E-mail and personal information in the address book and calendar that resides on our network is duplicated to our Blackberries. Therefore, Blackberry units should also have password protection. We strongly encourage all Blackberry users to enable security on their units. This way, if the unit is ever lost or stolen, it will not be a window into the Firm's email system or your personal information. In due course, we expect to be able to implement a policy under which all Blackberries will be password protected and Blackberry passwords would need to be changed every six months.

To set the password on your Blackberry:

1. From the menu on your Blackberry, using the wheel, scroll until you highlight the "Options" icon.
2. Select "Options" by depressing the wheel.
3. Using the wheel, scroll to "Security" and select by depressing the wheel.
4. Where it says Password, depress the wheel to select "Change Option." Use the wheel to change "Disabled" to "Enabled." Depress the wheel when "Enabled" is selected.
5. Type in your New Password and then depress the wheel; Type in the Password again and then depress the wheel.
6. Set the "Security Timeout" to 30 minutes (more or less depending on your preference). This feature automatically returns the Blackberry to the opening screen, requiring entering a password to re-enter, after a designated time period. To do this, scroll the wheel to "Security Timeout," depress the wheel; scroll to "Change Option" and depress the wheel again. Scroll down until the time period reads 30 min (or whatever time you select) and depress the wheel.
7. To Save, press down on the wheel, Scroll to Save Options, depress the wheel to save.

We trust that you will understand the need to impose the password requirements on all system users. We must do all we can to strengthen our system's security, to save you some effort, **please do not ask for any exceptions to the policy. They will not be granted.**

Email

The Firm provides the necessary software and systems to support electronic communication both within the Firm and with others outside the Firm. The use of the email system is solely for the purpose of conducting business, however, the Firm recognizes that limited, occasional or incidental use of email for personal, non-business use is acceptable, so long as it does not interfere with the employee's productivity or otherwise violate this or any other Firm policy in effect from time to time. Email sent outside the Firm for non-Firm related business should be minimal so as to not impact the Firm's systems. Email communications within the system and through the Internet are the property of the Firm, and are monitored.

All email sent outside of the Firm must include the Firm's standard disclaimer statement.

Proper email etiquette should be used at all times. Standard business codes of conduct should be used. Email may not be used for knowingly transmitting, retrieving or storing communications

- of a discriminatory or harassing nature
- that are derogatory to any individual or group
- that are obscene or "x-rated"
- of a defamatory or threatening nature
- in the form of "chain letters"
- that divulge trade secrets or other confidential information of the Firm or its clients
- that are illegal or against Firm policy or contrary to the Firm's interest

Inbound email containing programs, pictures, or other non-business related material will in most cases be blocked by the Firm's firewall. Any items passed through the firewall should be deleted upon receipt if non-business related.

Because of potential liability to the employee and to the Firm, the content of email is subject to control and monitoring by *FIRM NAME*. The Firm reserves the right, in its discretion, to review any employee's electronic messages and usage to the extent necessary to ensure that email is being used in compliance with the law and with this and other Firm policies. Since all emails are the property of *FIRM NAME*, employees must realize that they should have no expectation of privacy in their email communications, even if they are personal messages from employee to employee or from employee to an outside contact, via the Internet. All messages are subject to review by management and all communications are subject to scrutiny, even if the messages are consensual or personal in nature.

The Firm's policy regarding the retention of email on the system is as follows: Messages in the Inbox (including folders) are kept indefinitely or until you delete them. Sent items (including folders) are kept indefinitely or until you delete them. Deleted items (not in folders) are kept for 30 days before being purged from the system. It is the responsibility of the employee to ensure that important messages and attachments are filed electronically to the LegalKey Records Management system by using LKSend, or by printing out a hard copy of the email message and sending it to the file room.

Retention of Electronic Client Records

Advances in the technology used to aid in the practice of law have impacted the way we do business. One of the most significant changes is in the manner of delivering information to one another, and to those outside the Firm. Increasingly, we are transmitting information electronically through e-mail and desktop faxing. Most of these communications constitute client records, which we have an ethical obligation, as well as a practical need, to maintain. As we upgrade our computer system, storage and retrieval of electronic communications will become more sophisticated, and we will develop ways to retain this information in automated systems where it will be accessible and easily retrieved. Until then, however, we must take all reasonable steps to assure that our clients' records are complete.

To assure that all work-related information that comes into the possession of a *FIRM NAME* attorney becomes part of the client's file, all lawyers are expected to send, or cause to be sent, hard copies of hard and electronic documents (e.g., e-mail, correspondence, faxes, notes) to the Records Department for indexing in the Legal Key Records Management system and filing in the "official" files. As a further safeguard, effective immediately and until further notice, the following guidelines should be followed:

- Do not delete e-mail messages pertaining to client matters from the system.
- Do not delete documents attached to e-mail messages from the system.

We recognize that some messages (whether sent electronically or in a more traditional form) are not substantive, and have no lasting significance. Communications of that type do not need to be preserved. Attorneys should use their judgment to determine whether a particular document needs to be retained in the files. When in doubt, please err on the side of retaining the documents.

To support this policy change you should declare client related emails and attachments to LegalKey using LKDeclare. The messages can be searched and retrieved by client and matter number using LKSearch from within Outlook. As part of an overall review of document retention policies and procedures for the Firm, a workgroup consisting of certain lawyers, staff and IT and Records personnel has been commissioned. This group will identify best practices in the area and will recommend a policy for approval by the Executive Committee with consideration being given to legal and ethical obligations of the Firm and practical considerations of working lawyers and staff.

Virus Protection

The Firm provides the necessary software within its systems to guard against computer viruses. However, computer viruses are easily developed and spread via email systems, which makes the detection of every virus nearly impossible. It should not be assumed that typical sources of documents and other types of files such as clients or co-counsel are "trusted" sources. These sources are often just as vulnerable to virus attacks as is the Firm.

The Firm virus detection system functions in one of two ways. It cleans infected files as they come into our system and moves a clean version to the intended recipient, or if it

cannot clean the infected file, it removes it from the system and notifies the sender and the recipient. If you identify a virus-infected document you are strongly encouraged to contact the sender and advise them that this has happened.

Internet

Internet access is unrestricted to provide the highest level of service to the Firm. The fact that access is unrestricted requires that the Internet be used appropriately.

The Internet should be used for client-related activities. As with the use of Email, the Firm recognizes that limited, occasional or individual use of the Internet is acceptable so long as it does not interfere with the business of the Firm.

Internet access should not be used to conduct business or for activities not related to clients or potential clients of the Firm. This includes but is not limited to electronic stock trading, electronic auctions, games, on-line gambling, Internet Radio, downloading, and/or playing digital music, bulletin boards, listservs and posting of messages not related to client activities.

Attorneys and Staff must presuppose that all materials on the Internet are copyright and/or patented unless specific notices state otherwise. Downloading and storing copyright material on firm equipment is prohibited.

Bandwidth both within the firm and in connecting to the Internet is a shared, finite resource. Everyone must make reasonable efforts to use this resource in ways that do not negatively affect others.

Adult content sites are strictly prohibited.

Compliance by Employees

Any employee found to be violating the Firm's policies on the proper use of electronic media will be subject to disciplinary action, up to and including termination.