DATA SECURITY POLICY

RISK MANAGEMENT PRACTICE GUIDE OF LAWYERS MUTUAL

LAWYERS MUTUAL | LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

www.lawyersmutualnc.com

LAWYERS MUTUAL LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

919.677.8900 | 800.662.8843 | www.lawyersmutualnc.com

OCTOBER 2016

Data Security Policy

RISK MANAGEMENT PRACTICE GUIDE OF LAWYERS MUTUAL

TABLE OF CONTENTS

INTRODUCTION

With each new piece of technology comes new potential for data security breach. The dangers inherent in using a smartphone or tablet are quite different from those associated with a laptop. Even the convenience of wireless internet has more opportunities for attack than traditional hard-wired systems. While most security measures focus on external threats from hackers and malicious downloads, internal threats account for twice as much monetary loss as external threats. An internal threat could be the deletion or dissemination of computer files related to a client's case. One employee could also share their password with another, granting someone access beyond the scope of their position.

To prevent the intentional or unintentional problems created by employee use of software and equipment, developing a thorough data securities policy is more important than ever. This policy should provide employees with information regarding the acceptable use of mobile technology as well as password security and wireless access policies to protect confidential data.

“While most security measures focus on external threats from hackers and malicious downloads, internal threats account for twice as much monetary loss as external threats.”

ELEMENTS OF A DATA SECURITY POLICY

A law firm depends on protecting confidential client information. Most of this information is available in electronic format for accessibility in and out of the office. Preventing client information from mysteriously growing legs or disappearing is crucial to a law firm's well-being.

❶ Office Computers and Server

There are some truths that should be self-evident but need to be spelled out in a written policy, because inevitably an employee will otherwise do the unthinkable. Some may ignore the Not Safe for Work (NSFW) tag and view pornography if they are 'off the clock' during a break or lunch hour, while others may decide to run a personal business or game server using the firm's servers. Both of these activities expose the office to security risks.

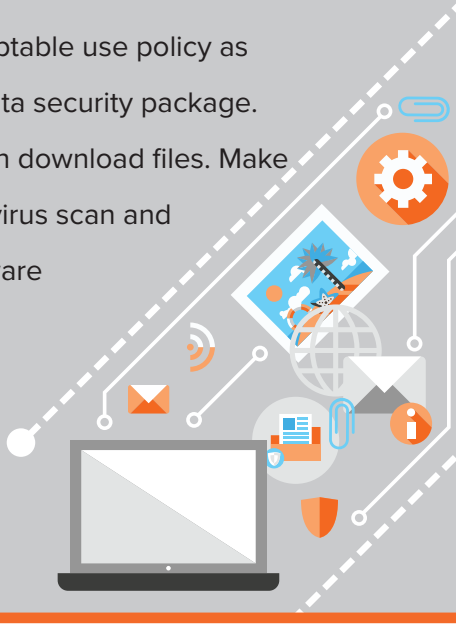
Some less obvious but equally risky behavior is the desire to download software from the internet onto company computers and/or servers. An employee could simply be looking for a tool to make them more efficient in their job. However, looking in the wrong place and downloading the wrong file could install malicious software onto your system.

Perhaps the scariest danger is the easiest one to complete: deleting files. Deleting a file can sometimes be as simple as hitting the wrong key combination, resulting in a mad dash to the IT specialist with the order to "retrieve!" said file from the trash bin. On those occasions that the deletion wasn't noticed right away, IT can spend a significant amount of time with the backup locating the document to hopefully restore it.

To prevent these and other related computer and server nightmares, create an acceptable use policy as part of your data security package. Restrict who has the right to download executable files (programs) and who can modify items in certain folders. Firewalls, virus scan and anti- spam software should be installed, updated and the system regularly scanned.

DATA-SECURITY TIPS

Create an acceptable use policy as party of your data security package. Restrict who can download files. Make sure you have virus scan and anti-spam software installed.



❷ Secure Backups

Is losing a day's worth of work acceptable, let alone a week? Backing up the office servers every night and storing that data off-site can save a law firm. Disasters don't wait for you to be prepared before they strike. Servers, like other computers, can die without warning. Having a full backup available allows you to upload your data onto a new server (after a new server is acquired and built) and continue working without having to reinvent lost work. It's even better when you have a redundant system, and you can simply switch to your backup server and continue on as if nothing has happened.

There are different varieties of backup systems available. Cloud backups remove the need for equipment but require extra vigilance regarding security when selecting a company. USB backups give the convenience of a portable backup, but proper security must be maintained since they are small and easily lost. Older tape backups require special equipment, someone diligently managing the process, and secure storage.

When planning your backup system, budget may be a factor in deciding which route you take. However, you have to pick a system you will use. Saving money isn't a value if it's tedious work that never actually gets done and you don't have a current backup when you need it.

Your backup policy should include determination for how long backup copies will be kept. Additional USB drives can be purchased to maintain offsite backups. If using the tape system, have a series of tapes that you rotate. Because tapes deteriorate, replace them on a regular basis to prevent problems. Keeping end of month or end of year backups offsite may be helpful as well.

❸ Password Security

Recent headlines highlight the continued problem of creating simple passwords that are quickly hacked because they are easier to remember. If a site requires a complicated password, some people will write it down and attach the post-it note to their computer so they have easy access to it when they need it. Others save a document in the system with their list of passwords to various sites. Any of these methods are hazards that can provide unauthorized access to your system.

To combat the dangers of password accessibility, provide minimum requirements of at least eight characters and combinations of the following: lowercase letters, uppercase letters, numbers, and special characters. Simple common words or the individual's name and date of birth should be prohibited. Provide some examples of possible strong passwords that would be easy to remember, such as word combinations (previous addresses: Main#202ParkDrive). Passwords should be scheduled to be changed on a regular basis, and passwords should not be able to be used over and over again in succession.

In addition to making sure individual passwords are truly secure, be sure that the system passwords for wireless access and other equipment are also changed. These hidden passwords can open up the entire system to hackers even if you think you've created a secure system with layers of access.

❹ Internet Use

Preventing employees from ever surfing to a non-work-related website can be cost prohibitive for small and medium sized firms. However, having a clear internet use policy can help limit the types of sites they visit. Streaming music and video use a lot of bandwidth, and downloaded files from filesharing sites can contain malware or expose the firm to liability if material was copyrighted. Some employees may be tempted to spend too much time on activities such as online shopping, social media or travel planning,

Again, use the theory that if it isn't forbidden, they will do it. Specifically list any types of sites that you do not want your employees visiting on your office computer. Security settings can be set to block porn sites, gambling sites, social media and even web-based email sites.

DATA-SECURITY TIPS. Make sure you have a clear **internet use policy** which can limit the types of sites your employees visit. Streaming music and video uses a lot of bandwidth and downloading files can expose you to malware or copyright issues.

The logic behind blocking personal, web-based email is prevention of employees from opening emails and visiting a nefarious site or opening an infected attachment, thereby compromising your system because their personal email was not as secure. Employees may inadvertently or maliciously transmit client confidential or law firm proprietary information using their personal webmail, circumventing other safeguards the firm has established concerning such information. Remind employees that, like email, browsing history is subject to being reviewed.

DATA-SECURITY TIPS

Email policies are extremely important.

1. Can employees use company email for personal business?
2. Does your policy limit attachment size?
3. What is your e-mail retention policy?

5 E-mail

Misuse of company email is one of the most common problems faced, and covers a large variety of actions. Sending a free "Happy Birthday!" card from a free website can introduce massive spamming into your system and bog down your server. Employees may use company e-mail for running a personal business with less thought than storing hard files on the computers or servers. A good Samaritan employee may send out emails to everyone in the firm regarding a fundraising event for a local charity, and follow up with four or five reminders. Personal use of the firm email system should be addressed to reduce the amount of server space such items consume.

E-mail policies should also include limits on the size of attachments as appropriate. Consider this: an e-mail with a 10MB attachment is received and then forwarded to ten other employees. This attachment now consumes 120MB of server space as each individual copy of the e-mail is stored on the server, plus the copy in the sent folder. Depending on your e-mail client, a copy of the e-mail may also be stored on each and every computer.

The above space consumption issue illustrates the reasoning behind another policy: e-mail retention policy. Case-related e-mails and attachments should be uploaded into a practice management system or database, protecting them from accidental deletion and making them accessible to all employees who may need the information. Storing emails that need to be saved outside of the e-mail system also prevents the dreaded moment when the recipient is out of the office and IT has to search their e-mail so another employee can access the information.

An essential element of an e-mail policy is reminding employees that the office email system is firm property and not their personal account. As such, any office email account is subject to review. Remind employees that office e-mail is representative of the firm and should present a professional image.

6 Metadata

Perhaps the most overlooked data security danger is metadata contained in document editing programs. Both Microsoft Word and WordPerfect contain information regarding previous edits made to a document. This means that deleting confidential information from one client document to reuse for

another could expose the former client's information to the latter if the recipient knows where to look. These features can be turned off, preventing data from being stored in the first place.

Files sent electronically should be scrubbed for metadata. Special programs can be purchased to ensure that this information is not forwarded along with your document and can be integrated into your email system. If you do not want the recipient to make changes to your document, send the document as a PDF. Sending as a PDF strips most of the metadata from a file, but a PDF contains some of its own. Be sure to adjust the security options as appropriate.

7 Remote Access

Employees may need to access the firm's system when they are out of the office occasionally. Prohibiting employees from using public computers or using wireless access in public places removes the exposure of client data from hackers because security settings in these circumstances are often lower than those created for the office.

To make connecting to the office more secure, consider establishing a virtual private network (VPN). A VPN connects you to your office computer over the internet, alleviating the need to actually access files through a questionable internet connection. Communications sent through the VPN are encrypted, so any data intercepted would not be usable.

8 Smartphones, Tablets and Remote Storage Devices

The trickiest part of data security is protecting the mobile data that leaves the building. Smartphones and tablets all contain internet connections but often do not have all of their security measures activated as a firm laptop would provide. A USB drive often contains pure, unencrypted files available for anyone who plugs the drive into their computer; worse yet, it is small enough to easily lose.

Any device used to access client data should have password protection requirements. Even a USB device can be purchased that requires password access. For smartphones and tablets, require passwords at start up and after a period of idle time. Also, develop a remote wipe program protocol should any device ever be lost or stolen. Any document downloaded and stored should be encrypted. When travelling, be careful not to leave your device in 'airplane mode' as this often disables the ability to enact a remote wipe program as it disconnects the device from data systems used to locate it.

Upon return to the office, require that remote storage devices such as USB and flash drives be scanned by virus and malware scanners to prevent infection from any outside sources. Have protocols in place regarding the use of personal USB devices with office computers to avoid inadvertently infecting office computers with unprotected devices. Consider restricting access to USB ports to certain employees, or even disable ports to prevent misuse.

“

The trickiest part of data security is protecting the mobile data that leaves the building. Smartphones and tablets all contain internet connections but often do not have all of their security measures activated as a firm laptop would provide.

WHEN AN EMPLOYEE LEAVES

Often the biggest threat to your data is within your own company. A disgruntled or exiting employee can easily delete files from your system or take files out of the office without notice. Locking down data from employees can be the hardest part of data security.

When an employee leaves, immediately lock their computer, e-mail, remote access and any other access privilege to prevent them from accessing information. Create protocols within the firm for who may need to access an employee's files. If the employee has any equipment, such as a laptop or USB drive, at home, verify that it is returned before they exit the premises on their final day.

DATA-SECURITY TIPS

Do you know what to do when an employee leaves?

One of the biggest threats to your data is wthin your own company. An exiting or disgruntled employee can easily delete files from your system.

VISITORS AND CONTRACTORS

From time to time, office visitors may need to use office computers or email. Any temporary account established should have a notice regarding expectation of privacy. Passcodes for these accounts should also expire immediately after use. This ensures someone temporarily allowed into your system won't be able to access your confidential data later, when you're not looking.

System contractors obviously need access to keep everything up-to-date and running smoothly. However, they may not understand the importance of the confidentiality of the information they may access in the process of completing their work. A Vendor/ Contractor Confidentiality Agreement should be completed by all of those who will be accessing your system to ensure that confidentiality is maintained.

SECURITY AUDIT

To ensure all facets of your system are properly secure, consider a third party secuity audit. A trained professional will see any holes in your protection that could leak confidential information.

The auditor will be able to provide you with suggestions to improve your security to prevent data security breaches in the future. This may include the purchase of additional security software, or simply changing internet usage habits. The end result will be a safer practice.

SAMPLE POLICY TABLE OF CONTENTS

I. OVERVIEW

a. Purpose - <Firm Name> is entrusted with the responsibility to provide professional legal advice to clients who provide us with confidential information. Inherent in this responsibility is an obligation to provide appropriate protection against theft of data and malware threats, such as viruses and spyware applications. The purpose of this policy is to establish standards for the base configuration of equipment that is owned and/or operated by <Firm Name> or equipment that accesses <Firm Name>'s internal systems. Effective implementation of this policy will minimize unauthorized access to <Firm Name> proprietary information and technology and protect confidential client information.

b. Scope - This policy applies to equipment owned and/or operated by <Firm Name>, and to employees connecting to any <Firm Name>-owned network domain.

II. NETWORK/SERVER SECURITY

a. Server Configuration Guidelines
   i. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
   ii. Servers should be physically located in an access-controlled environment.
   iii. Servers are specifically prohibited from being operated from uncontrolled cubicle areas.

b. Security-related Events - Security-related events will be reported to the IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
   i. Port-scan attacks
   ii. Evidence of unauthorized access to privileged accounts
   iii. Anomalous occurrences that are not related to specific applications on the host.

c. Router Security
   i. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
   ii. Disallow the following:
      1. IP directed broadcasts
      2. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
      3. TCP small services
      4. UDP small services
      5. All source routing
      6. Web services running on router
   iii. Access rules are to be added as business needs arise.
   iv. Each router must have the following statement posted in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

d. Server Malware Protection
   i. Anti-Virus - All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:
      1. Non-administrative users have remote access capability
      2. The system is a file server
      3. Share access is open to this server from systems used by non-administrative users
      4. HTTP/FTP access is open from the Internet

5. Other "risky" protocols/applications are available to this system from the Internet at the discretion of the <Firm Name> IT department.

ii. Mail Server Anti-Virus - If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound e-mails while the backup is being performed.

iii. Anti-Spyware - All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:
   1. Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
   2. Any system where non-technical or non-administrative users have the ability to install software on their own

iv. Notable Exceptions - Exceptions to above requirements may be deemed acceptable with proper documentation if one of the following notable conditions applies to this system:
   1. The system is a SQL server
   2. The system is used as a dedicated mail server
   3. The system is not a Windows based platform

e. Backup Procedures

i. Daily Backups - Backup software shall be scheduled to run nightly to capture all data from the previous day.
   1. Backup logs are to be reviewed to verify that the backup was successfully completed.
   2. One responsible party should be available to supervise backups each day. If the designated backup specialist is not available, an alternative should be named to oversee the process.

ii. Backup data storage shall not be on the <Firm Name>'s premises. In case of a disaster, backup tapes should be available for retrieval and not subject to destruction.

iii. Data on hard drives will be backed up daily, and mobile devices shall be brought in to be backed up on a weekly basis or as soon as practical if on an extended travel arrangement.

iv. Test restoration process regularly and create written instructions in the event IT personnel are not available to restore data when needed.

III. WORKSTATION SECURITY

a. Authorized Users - Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorized users.

b. Safeguards - <Firm Name> will implement physical and technical safeguards for all workstations that access electronic confidential information to restrict access to authorized users. Appropriate measures include:

i. Restricting physical access to workstations to only authorized personnel.

ii. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.

iii. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.

iv. Complying with all applicable password policies and procedures.

v. Ensuring workstations are used for authorized business purposes only

vi. Never installing unauthorized software on workstations.

vii. Storing all confidential information on network servers.

viii. Keeping food and drink away from workstations in order to avoid accidental spills.

ix. Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.

x. Complying with the Portable Workstation Encryption policy.
xi. Complying with the Anti-Virus policy.
xii. Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
xiii. Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
xiv. Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
xv. If wireless network access is used, ensure access is secure by following the Wireless Access policy.

c. Software Installation
   i. Employees may not install software on <Firm Name's> computing devices operated within the <Firm Name> network. Software requests must first be approved by the requester's manager and then be made to the IT department in writing or via e-mail. Software must be selected from an approved software list, maintained by the IT department, unless no selection on the list meets the requester's need. The IT department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.
   ii. This policy covers all computers, servers, and other computing devices operating within <Firm Name>'s network.

d. Malware Protection
   i. Anti-Virus - All <Firm Name> computers must have <Firm Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into <Firm Name>'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use policy.

IV. PASSWORD SECURITY

a. Requirements
   i. All system-level passwords (Administrator, etc.) must be changed on a quarterly basis, at a minimum.
   ii. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
   iii. All user-level and system-level passwords must conform to the standards described below.

b. Standards - All users at <Firm Name> should be aware of how to select strong passwords. Strong passwords have the following characteristics:
   i. Contain at least three of the five following character classes:
      1. Lower case characters
      2. Upper case characters
      3. Numbers
      4. Punctuation
      5. "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
   ii. Contain at least eight to fifteen alphanumeric characters.
   iii. The password is NOT a word found in a dictionary (English or foreign).
   iv. The password is NOT a common usage word such as:
      1. Computer terms and names, commands, sites, companies, hardware, software. Passwords should NEVER be "Password1" or any derivation.
      2. The words "<Firm Name>", "<City>", or any derivation.
      3. Names of family, pets, friends, co-workers, etc.

4. Birthdays and other personal information such as addresses and phone numbers.
5. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
6. Any of the above spelled backwards.
7. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

v. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.

c. Protective Measures
   i. Do not share <Firm Name> passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential <Firm Name> information.
   ii. Passwords should never be written down or stored on-line without encryption.
   iii. Do not reveal a password in email, chat, or other electronic communication.
   iv. Do not speak about a password in front of others.
   v. Do not hint at the format of a password (e.g., "my family name").
   vi. Do not reveal a password on questionnaires or security forms.
   vii. If someone demands a password, refer them to this document and direct them to the IT Department.
   viii. Always decline the use of the "Remember Password" feature of applications.
d. Passphrases - Access to the <Firm Name> Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.
   i. A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "Joe&Me1RBudz"
   ii. All of the rules above that apply to passwords apply to passphrases.

V. ACCEPTABLE USE

a. General Use and Ownership
   i. While <Firm Name>'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of <Firm Name>.
   ii. Any information that users consider sensitive or vulnerable be encrypted.
   iii. For security and network maintenance purposes, authorized individuals within <Firm Name> may monitor equipment, systems and network traffic at any time.
b. Security and Proprietary Information
   i. The user interface for information contained on <Firm Name>'s systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines. Employees should take all necessary steps to prevent unauthorized access to this information.
   ii. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
   iii. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when unattended.
   iv. All PCs, laptops and workstations used by the employee that are connected to the <Firm Name> network, whether owned by the employee or <Firm Name>, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
   v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
c. Unacceptable Use
   i. The following activities are, in general, prohibited. The lists below are by no means exhaustive, but

attempt to provide a framework for activities which fall into the category of unacceptable use.

1. Under no circumstances is an employee of <Firm Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Firm Name>-owned resources.
2. Violations of the rights of any person or Firm protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <Firm Name>.
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Firm Name> or the end user does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a <Firm Name> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any <Firm Name> account.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the IT department is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet.
15. Providing information about, or lists of, <Firm Name> employees to parties outside <Firm Name>.

d. Wireless Access

   i. <Firm Name> Device Requirements - All wireless devices that reside at a <Firm Name> site and connect to a <Firm Name> network must:

      1. Be installed, supported, and maintained by the IT department.
      2. Use <Firm Name> approved authentication protocols and infrastructure.
      3. Use <Firm Name> approved encryption protocols.
      4. Maintain a hardware address (MAC address) that can be registered and tracked.

   ii. Home Wireless Device Requirements

      1. Wireless devices that provide direct access to the <Firm Name> corporate network, must conform

to the security protocols as detailed for <Firm Name> wireless devices.

2. Wireless devices that fail to conform to security protocols must be installed in a manner that prohibits direct access to the <Firm Name> corporate network. Access to the <Firm Name> corporate network through this device must use standard remote access authentication.

VI. ENCRYPTION

a. Standards - Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Key lengths must be at least 128 bits. <Firm Name>'s key length requirements will be reviewed annually and upgraded as technology allows.

b. Mobile Device Encryption

   i. Scope - All mobile devices containing stored data owned by <Firm Name> must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, tablets, and smartphones.

   ii. Laptops - Laptops must employ full disk encryption with an approved software encryption package. No <Firm Name> data may exist on a laptop in cleartext.

   iii. Tablet and smartphones - Any <Firm Name> data stored on a smartphone or tablet must be saved to an encrypted file system using <Firm Name>-approved software. <Firm Name> shall also employ remote wipe technology to remotely disable and delete any data stored on a <Firm Name> tablet or smartphone which is reported lost or stolen.

   iv. Keys - All keys used for encryption and decryption must meet complexity requirements described in <Firm Name>'s Password Security policy.

VII. E-mail

a. Prohibited Use - <FIRM NAME> e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any e-mails with this content from any <FIRM NAME> employee should report the matter to their supervisor immediately. The following activities are strictly prohibited, with no exceptions:

   i. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

   ii. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.

   iii. Unauthorized use, or forging, of e-mail header information.

   iv. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

   v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

   vi. Use of unsolicited e-mail originating from within <Firm Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Firm Name> or connected via <Firm Name>'s network.

   vii. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

b. Personal Use - Using a reasonable amount of <FIRM NAME> resources for personal e-mails is acceptable, but nonwork related e-mail shall be saved in a separate folder from work related e-mail. Sending chain letters or joke e-mails from a <FIRM NAME> e-mail account is prohibited. Virus or other malware warnings and mass mailings from <FIRM NAME> shall be approved by <FIRM NAME> IT department before sending. These restrictions also apply to the forwarding of mail received by a <FIRM NAME> employee.

c. E-mail Retention
   i. Administrative Correspondence - <Firm Name> Administrative Correspondence includes, though is not limited to clarification of established Firm policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All e-mail with the information sensitivity label Management Only shall be treated as Administrative Correspondence. <Firm Name> Administration is responsible for e-mail retention of Administrative Correspondence.
   ii. Fiscal Correspondence - <Firm Name> Fiscal Correspondence is all information related to revenue and expense for the Firm. <Firm Name> bookkeeper is responsible for all fiscal correspondence.
   iii. General Correspondence - <Firm Name> General Correspondence covers information that relates to customer interaction and the operational decisions of the business. <Firm Name> is responsible for e-mail retention of General Correspondence.
   iv. Ephemeral Correspondence - <Firm Name> Ephemeral Correspondence is by far the largest category and includes personal e-mail, requests for recommendations or review, e-mail related to product development, updates and status reports.
   v. Encrypted Communications - <Firm Name> encrypted communications should be stored in a manner that protects the confidentiality of the information, but in general, information should be stored in a decrypted format.
   vi. Recovering Deleted E-mail via Backup Media - <Firm Name> maintains backups from the e-mail server and once a quarter a set of backups is taken out of the rotation and they are moved offsite. No effort will be made to remove e-mail from the offsite backups.

d. Monitoring - <FIRM NAME> employees shall have no expectation of privacy in anything they store, send or receive on the Firm's e-mail system. <FIRM NAME> may monitor messages without prior notice. <FIRM NAME> is not obliged to monitor e-mail messages.

VIII. METADATA

a. Definition - When you create and edit your documents, information about you and the edits you make is automatically created and hidden within the document file. Metadata can often be sensitive or confidential information, and can be potentially damaging or embarrassing. On its Web site, Microsoft indicates that the following metadata may be stored in documents created in all versions of Word, Excel and PowerPoint:
   i. your name and initials (or those of the person who created the file)
   ii. the name of your computer
   iii. your firm or organization name
   iv. the name and type of the printer you printed the document on
   v. document revisions, including deleted text that is no longer visible on the screen
   vi. document versions
   vii. information about any template used to create the file
   viii. hidden text
   ix. comments

b. Removing Metadata
   i. Microsoft
      1. Disable "allow fast saves" feature.
      2. "Inspect Document" and remove flagged items. "Inspect Document" will vary depending on your software version. In 2010, it is located under File->Info->Check For issues.
      3. Third party software will help identify and clean metadata from your documents if it is necessary to send documents in native format. Verify appropriate software with the IT department.
   ii. WordPerfect

1. Uncheck Save Undo/Redo items with document. It can allow you to view hundreds of past changes in terms of what text was cut, copied and even deleted from the document.
2. There is no software program that easily and automatically removes metadata from WordPerfect documents.

iii. Converting to PDF

1. Converting files to PDF format with Adobe Acrobat or other PDF creators will usually strip out most metadata.
2. In Acrobat, Select File, then Document Properties to view the summary metadata information within a PDF file. Add further restrictions on how the document can be accessed, used, copied and printed in the Security Options settings as needed.

IX. REMOTE ACCESS

a. Persons Affected - <FIRM NAME> employees, consultants, vendors, contractors, students, and others who use mobile computing and storage devices on the network at the <FIRM NAME>.

b. General Standards - It is the responsibility of <Firm Name> employees, contractors, vendors and agents with remote access privileges to <Firm Name>'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Firm Name>.

c. Requirements

i. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password policy.

ii. At no time should any <Firm Name> employee provide their login or e-mail password to anyone, not even family members.

iii. <Firm Name> employees and contractors with remote access privileges must ensure that their <Firm Name>-owned or personal computer or workstation, which is remotely connected to <Firm Name>'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

iv. <Firm Name> employees and contractors with remote access privileges to <Firm Name>'s corporate network must not use non-<Firm Name> e-mail accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct <Firm Name> business, thereby ensuring that official business is never confused with personal business.

v. Routers configured for access to the <Firm Name> network must meet minimum authentication requirements .

vi. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

vii. Non-standard hardware configurations must be approved by the IT department, and <Firm Name> must approve security configurations for access to hardware.

viii. All PCs, laptops and workstations that are connected to <Firm Name> internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers.

ix. Personal equipment that is used to connect to <Firm Name>'s networks must meet the requirements of <Firm Name>-owned equipment for remote access.

x. Individuals who wish to implement non-standard Remote Access solutions to the <Firm Name> production network must obtain prior approval from the IT department.

d. Mobile Computing and Storage Devices

i. Items covered - Mobile computing and storage devices include, but are not limited to: laptop computers,

plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or <Firm Name> owned, that may connect to or access the information systems at the <FIRM NAME>.

ii. Risks - Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at the <FIRM NAME>. These risks must be mitigated to acceptable levels.

iii. Encryption - Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive <FIRM NAME> information must use encryption or equally strong measures to protect the data while it is being stored.

iv. Database - Databases or portions thereof, which reside on the network at the <FIRM NAME>, shall not be downloaded to mobile computing or storage devices.

v. Minimum Requirements:

1. Report lost or stolen mobile computing and storage devices to the IT department.
2. Non-departmental owned device that may connect to the <FIRM NAME> network must first be approved by the IT department.
3. Compliance with the Remote Access policy is mandatory.

e. Virtual Private Network (VPN)

i. Persons affected - This policy applies to all <Firm Name> employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the <Firm Name> network.

ii. Connectivity - Approved <Firm Name> employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

iii. Requirements

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to <Firm Name> internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by <Firm Name>'s IT department.
6. All computers connected to <Firm Name> internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from <Firm Name>'s network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not <Firm Name>-owned equipment must configure the equipment to comply with <Firm Name>'s VPN and Network policies.
10. Only <Firm Name>-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of <Firm Name>'s network, and as such are subject to the same rules and

regulations that apply to <Firm Name>-owned equipment, i.e., their machines must be configured to comply with <Firm Name>'s Security Policies.

X. Employee Termination
   a. Removing access - An employee's credentials shall be inactivated immediately upon termination of employment. This includes, but is not limited to the following:
      i. <Firm Name's> database
      ii. Workstation access
      iii. E-mail access
      iv. Remote access to <Firm Name>'s network
      v. VPN client access
      vi. Any other access to <Firm Name>'s network or programs
   b. Returning mobile devices - Any employee in possession of firm portable devices shall return such devices before exiting the premises on their final day of employment. Mobile devices include, but are not limited to, the following:
      i. <Firm Name>-owned smartphone
      ii. <Firm Name>-owned tablet
      iii. Laptop
      iv. USB drive
      v. CD or DVD containing <Firm Name> client information

XI. Visitor and Contractor Access
   a. Permission - Visitors who require internet network access will need permission the IT department. After credentials are arranged, activities on the network will be subject to the Acceptable Use policy. Visitor use of employee credentials is not permitted under any circumstances.
   b. Contractors - Contractors making changes to the network should notify the IT department if any interruption of services is anticipated. Prior arrangement should be made to notify all staff of the interruption if possible.
   c. Remote Access - Remote Access to <Firm Name> networks are governed by the <Firm Name> Remote Access policy.

XII. Enforcement
   a. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

SERVICE PROVIDER CONFIDENTIALITY AGREEMENT

It is the policy and practice of _____(hereinafter "the firm") that the confidentiality of all client, law office business and related matters is carefully guarded and protected in every possible and reasonable manner at all times. For that reason, you are being asked in your capacity as an employee or representative of "X ", a service provider to "the firm" (hereinafter "X") to review and sign this confidentiality form. Your signature below represents and documents your acknowledgement and agreement to maintain complete and strict confidentiality regarding any client information and any and all other office matters that you may be told or inadvertently or otherwise learn in the course of your work with "Law Firm."

Any breach of this confidentiality policy to third parties will result in the immediate termination of our business relationship. Further, should you breach this confidentiality policy in any way, you and your company will be jointly and severally liable for any and all damages and expenses including attorney fees cause to "the firm," its clients or employees

I, _____, am an employee and authorized representative for "X" and have read, understand and agree to abide by the provisions of the foregoing stated policy.

Signed this _____ day of _____, 20___.

_____

courtesy of the Florida Bar

Additional Resources

INFORMATION SECURITY AND PRIVACY. Published by the American Bar Association. Available at www.abanet.org or by phone at 800.285.2221; product code 5450058. Price is $119.95 for members of the ABA.

MANAGING THE SECURITY AND PRIVACY OF ELECTRONIC DATA IN A LAW OFFICE. Published by Lawyers Professional Indemnity Company. Available at: http://www.practicepro.ca/practice/pdf/ManagingSecurityPrivacy.pdf

THREATS FROM WITHIN. By David Bilinsky. Published by The Law Society of British Columbia. Available at: http://www.lawsociety.bc.ca/docs/practice/resources/ThreatsFromWithin.pdf

Check out the following titles from the Lawyers Mutual Lending Library at: http://www.lawyersmutualnc.com/risk-management-resources/book-lending-library

CLOUD COMPUTING FOR LAWYERS.

ENCRYPTION MADE SIMPLE FOR LAWYERS.

LOCKED DOWN: INFORMATION SECURITY FOR LAWYERS.

THE ABA CYBERSECURITY HANDBOOK.