1-1-2022

Cybersecurity & Ethics for Lawyers in Plain English

Indiana Continuing Legal Education Forum (ICLEF)

Cybersecurity and Ethics for Lawyers in Plain English
April 26, 2022
Index

ICLEF Electronic Publications

Feature Release 4.1
August 2020

To get the most out of your *ICLEF Electronic Publication,* download this material to your PC and use Adobe Acrobat® to open the document. The most current version of the Adobe® software may be found and installed by clicking on one of the following links for either the free Adobe Acrobat Reader® or the full retail version of Adobe Acrobat®.

Feature list:

1. **Searchable** – All ICLEF Electronic Publications are word searchable. To begin your search, click on the "spyglass" icon at the top of the page while using the Adobe® software.
1. **Bookmarks** – Once the publication is opened using the Adobe Acrobat® software a list of bookmarks will be found in a column located on the left side of the page. Click on a bookmark to advance to that place in the document.
2. **Hypertext Links** – All of the hypertext links provided by our authors are active in the document. Simply click on them to navigate to the information.
3. **Book Index** – We are adding an INDEX at the beginning of each of our publications. The INDEX provides "jump links" to the portion of the publication you wish to review. Simply left click on a topic / listing within the INDEX page(s) to go to that topic within the materials. To return to the INDEX page either select the "INDEX" bookmark from the top left column or right-click with the mouse within the publication and select the words "*Previous View*" to return to the spot within the INDEX page where you began your search.

Please feel free to contact ICLEF with additional suggestions on ways we may further improve our electronic publications. Thank you.

Indiana Continuing Legal Education Forum (ICLEF)
230 East Ohio Street, Suite 300
Indianapolis, Indiana 46204
Ph: 317-637-9102 // Fax: 317-633-8780 // email: iclef@iclef.org
URL: https://iclef.org

CYBERSECURITY AND ETHICS FOR LAWYERS IN PLAIN ENGLISH

April 26, 2022

WWW.ICLEF.ORG

DISCLAIMER

The information and procedures set forth in this practice manual are subject to constant change and therefore should serve only as a foundation for further investigation and study of the current law and procedures related to the subject matter covered herein. Further, the forms contained within this manual are samples only and were designed for use in a particular situation involving parties which had certain needs which these documents met. All information, procedures and forms contained herein should be very carefully reviewed and should serve only as a guide for use in specific situations.

The Indiana Continuing Legal Education Forum and contributing authors hereby disclaim any and all responsibility or liability, which may be asserted or claimed arising from or claimed to have arisen from reliance upon the procedures and information or utilization of the forms set forth in this manual, by the attorney or non-attorney.

Attendance of ICLEF presentations does not qualify a registrant as an expert or specialist in any discipline of the practice of law. The ICLEF logo is a registered trademark and use of the trademark without ICLEF's express written permission is prohibited. ICLEF does not certify its registrants as specialists or expert practitioners of law. ICLEF is an equal opportunity provider of continuing legal education that does not discriminate on the basis of gender, race, age, creed, handicap, color or national origin. ICLEF reserves the right to refuse to admit any person or to eject any person, whose conduct is perceived to be physically or emotionally threatening, disruptive or disrespectful of ICLEF registrants, faculty or staff.

INDIANA CONTINUING LEGAL EDUCATION FORUM

OFFICERS

TERESA L. TODD
President

LYNNETTE GRAY
Vice President

HON. ANDREW R. BLOCH
Secretary

SARAH L. BLAKE
Treasurer

ALAN M. HUX
Appointed Member

LINDA K. MEIER
Appointed Member

DIRECTORS

James H. Austen
Sarah L. Blake
Hon. Andrew R. Bloch
Melanie M. Dunajeski
Lynnette Gray
Alan M. Hux
Dr. Michael J. Jenuwine
Shaunda Lynch
Thomas A. Massey
Linda K. Meier
Whittley Pike
Richard S. Pitts
Jeffrey P. Smith
Teresa L. Todd

ICLEF

SCOTT E. KING
Executive Director

James R. Whitesell
Senior Program Director

Jeffrey A. Lawson
Program Director

CYBERSECURITY AND ETHICS FOR LAWYERS IN PLAIN ENGLISH

Agenda

8:55 A.M. Welcome & Introduction

9:00 A.M. Cybersecurity & Ethical Pitfalls of Everyday Law Office Computing

Practicing anywhere at any time is no longer just a dream for lawyers, it's a reality. Under Model Rule 1.6 lawyers must take reasonable precautions to protect client info and data that is in their custody. We will discuss the ethical and malpractice pitfalls of mobile, cloud, and general everyday law office computing. We will learn about cloud storage options and address how to safely store documents and client and law firm data with cloud storage options like Dropbox, Box & OneDrive. We will finally discuss security vulnerabilities related to documents, emails and metadata associated with those files. We will also discuss how to properly delete client data, assign passwords, and dispose of computer equipment while protecting client privacy. (*Model Rule 1.1, Rule 1.6, Rule 5.3)*

10:30 A.M. Coffee break

10:45 A.M. Cybersecurity & Ethical Pitfalls of Everyday Law Office Computing (continued)

12:15 P.M. Lunch (on your own)

1:15 P.M. Centralizing and Securing Your Documents

Rule 1.6 stipulates that a lawyer must make reasonable efforts to prevent the disclosure of confidential client information. The comments to Rule 1.6 require lawyers to act competently to safeguard client information and use reasonable safety precautions when transmitting a client communication. The exact meanings of "reasonable efforts," "act competently" and "reasonable precautions" may be subject to debate. However, doing nothing certainly won't meet the standard. The good news is that you don't have to be a security expert or techie to protect yourself and your office. Learn how to centralize your firm and client data so you can properly govern and secure everything. Whether you access documents from a computer, laptop, or a mobile device, we'll cover all the bases on how to do it safely and securely. We'll also cover the fundamentals of backing up your electronic data. Half of the battle is simply knowing what questions to ask and it's not nearly as complicated as it sounds. Establish best practices in your office that will make sure your confidential information remains confidential. *(Model Rule 1.1, Rule 1.15, Rule 1.4, Rule 1.6)*

2:45 P.M. Break

Agenda Continued

3:00 P.M. Creating Your Firm's Cybersecurity & Disaster Avoidance Policy

Written Information Security Programs (WISPs) are becoming essential in many states that have enacted data protection and business shield legislation. Many cybersecurity insurance carriers covering lawyers are starting to require WISPs. Setting aside legislative and insurance requirements, under the Rules of Professional Conduct, lawyers still must implement safe technologies and processes to safeguard client confidential data. This is a very practical session where you will learn the essential elements of a Written Information Security Program. In this session, we will cover ransomware attacks, phishing schemes, cloud computing, mobile device management, full disk encryption, secure document management, shadow-IT, two-factor management, VPNs, anti-virus, backup, and law office support staff education
(Model Rule 1.1, Rule 1.15, Rule 5.3)

4:30 P.M. Adjournment

Faculty

Mr. Paul J. Unger
Affinity Consulting Group, LLC
1550 Old Henderson Road, Suite S-150
Columbus, OH 43220
ph: (614) 602-5572
e-mail: punger@affinityconsulting.com

Paul J. Unger, Affinity Consulting Group, LLC, Columbus, OH

Paul J. Unger is a nationally recognized speaker, author and thought-leader in the legal technology industry. He is an attorney and founding principal of Affinity Consulting Group, a nationwide consulting company providing legal technology consulting, continuing legal education, and training.

He is the author of dozens legal technology manuals and publications, including recent published books, *Tame the Digital Chaos – A Lawyer's Guide to Distraction, Time, Task & Email Management* (2017) and *PowerPoint in an Hour for Lawyers* (2014). He served as Chair of the ABA Legal Technology Resource Center (2012-13, 2013-14)(www.lawtechnology.org/), Chair of ABA TECHSHOW (2011)(www.techshow.com), and served as Planning Chair for the 2016 ACLEA Mid-Year Conference in Savannah, GA. He is a member of the American Bar Association, Columbus Bar Association, Ohio State Bar Association, Ohio Association for Justice, and New York State Bar Association, and specializes in document and case management, paperless office strategies, trial presentation and litigation technology, and legal-specific software training and professional development for law firms and legal departments throughout the United States, Canada and Australia. Mr. Unger has provided trial presentation consultation for over 400 cases. In his spare time, he likes to run and restore historic homes.

Cybersecurity and Ethical Pitfalls of Everyday Law Office Computing

*Paul J. Unger, Esq. (*punger@affinityconsulting.com*)*
Affinity Consulting Group

Protection of client information, confidences and secrets is one of the most sacred traits defining the relationship between lawyers and their clients. Without a proper understanding of technology, you may be compromising that relationship. Email, cloud computing, traditional computers, smartphones, tablets, networks, viruses, worms, spyware, metadata, electronic court filings, just to name a few, may already be compromising that relationship without you even knowing it.

Take email as an example. In 2022, the average legal professional will receive between 125-150 email messages daily and that doesn't include additional messages through applications like MS Teams or Slack. Without question, email is one of the most important technological communication advancements of the past 100 years. It has fundamentally changed the way we communicate with clients and the way that we do business. Major corporations and law firms are run via email communication instead of face-to-face communication. For lawyers, emails present a wide array of issues that most of the business world and ordinary consumers will never face.

In Canada and the U.S., lawyers have a duty to take reasonable steps to protect their client's confidential information, whether it is in the form of paper or electronic. Under ABA Model Rule 1.6, lawyers have a broad obligation to act competently and reasonably protect client information and confidences. Rule 1.6 (replacing DR 4-101) revised the scope of confidential information. Similarly, in Canada, Model Code of Professional Conduct, Rule 3.3 requires the same protection of client information and confidences. Practicing law without technology (and email) has almost become an impossibility.

However, law and technology have become so intertwined that you can find yourself in many ethical dilemmas pretty quick. This seminar and article seek to address these issues that may lead to an ethical violation or malpractice.

"Competence" Re-Defined and Taking Reasonable Steps to Protect Client Information

Trend in North America – Examples

The U.S. is not alone in requiring a lawyer to understand the benefits and risks of technology. On October 19, 2019, the Federation of Law Societies of Canada formally amended its Model Code to include the duty of technical competence. Comments to Rule 3.1-2 say:

> [4A] To maintain the required level of competence, a lawyer should develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice and responsibilities. A lawyer should understand the benefits and risks associated with relevant technology, recognizing the lawyer's duty to protect confidential information set out in section 3.3.
>
> [4B] The required level of technological competence will depend on whether the use or understanding of technology is necessary to the nature and area of the lawyer's practice and responsibilities and whether the relevant technology is reasonably available to the lawyer. In determining whether technology is reasonably available, consideration should be given to factors including:
>
> (a) The lawyer's or law firm's practice areas;
>
> (b) The geographic locations of the lawyer's or firm's practice; and
>
> (c) The requirements of clients.

Of course, individual Canadian provincial and territorial law societies still must adopt the rule, but that is anticipated over time. Like the U.S. the new language simply makes explicit what is already implied in the existing rules. Regardless, the act of making it explicit has clearly triggered a much higher awareness and we are seeing lawyers take significantly more steps to protect client electronically stored information.

Pennsylvania (approved October 22, 2013)

Rule 1.1 – Comment 8: Maintaining Competence
[8] To maintain the requisite knowledge and skill, a lawyer must keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Pennsylvania was the first state to adopt the new language. 38 states have adopted the Duty of Technical Competence. Some of those include:

Alaska (effective October 15, 2017)
Arkansas (effective June 26, 2014)
Arizona (effective January 1, 2015)
California (effect March 22, 2021)
Colorado (approved April 6, 2016)
Florida (effective January 1, 2017)
Indiana (effective January 1, 2018)
Illinois (effective January 1, 2016)
Kansas (effective March 1, 2014)
Kentucky (effective January 1, 2018)
Louisiana (adopted April 11, 2018)
Michigan (effective January 1, 2020)
Minnesota (approved February 24, 2015)
Missouri (approved Sept. 26, 2017)
New Hampshire (effective January 1, 2016)
New York (adopted March 28, 2015)
North Carolina (approved July 25, 2014)
Ohio (effective April 1, 2015)
Oklahoma (adopted September 19, 2016)
Pennsylvania (effective October 22, 2013)
South Carolina (approved November 27, 2019)
Virginia (effective March 1, 2016)
Washington (effective Sept.1, 2016)
West Virginia (effective January 1, 2015)
Wisconsin (effective January 1, 2017)

Some states have not yet adopted the new language within their rules of professional responsibility. As of February of 2021, those include:

Oregon
Nevada
South Dakota
Mississippi

Alabama
Georgia
Maine
Maryland
New Jersey

Some states have not adopted the rule change but have addressed it in an ethics opinion. For example, **Oregon** in Formal Opinion 2011-187 imposes a duty of technical competence *when dealing with metadata* and cites Arizona Ethics Op No. 07-03. It is reasonable to conclude that all Oregonian lawyers should have general technical competence (not just technical competence with metadata) in light of this opinion on metadata and the national trend.

Acting Competently to Preserve Confidentiality

Indiana Rule 1.6, Comments 16 & 17

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

Ohio Rule 1.6 (and Model Rule 1.6) and Comments 18 & 19

Rule 1.6(c) – Confidentiality of Information: A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Rule 1.6 – Comment 18 & 19: Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Similarly, many other states have taken the same approach in their comments, as the ABA and Ohio. Take Maine, New Hampshire and Oklahoma as an example:

Maine Rule 1.6
Acting Competently to Preserve Confidentiality – Comments 16 & 17

Acting Competently to Preserve Confidentiality

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. Consistent with Section 66 of the Restatement, a lawyer who takes action or decides not to take action allowed under this Rule is not, solely by reason of such action or inaction, subject to professional discipline, liable for damages to the lawyer's client or any third persons, or barred from recovery against a client or third persons. The legal effect of the lawyer's choice, however, is beyond the scope of the Model Rules of Professional Conduct.

[17] When transmitting a communication that includes confidences or secrets of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

New Hampshire Rule 1.6
Acting Competently to Preserve Confidentiality - Comments 18 & 19

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these rules.

Oklahoma Rule 1.6
Acting Reasonably to Preserve Confidentiality – Comments 16 & 17

[16] Paragraph (c) requires a lawyer to act reasonably to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern date privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3] -[4].

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Louisiana Rule 1.6 – Comments 18 and 19

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Mississippi Rule 1.6 + Comments

Mississippi requires reasonableness and competency, but they don't provide as much guidance in their comments as other states:

> **Acting Competently to Preserve Confidentiality.** A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See rules 1.1, 5.1 and 5.3.
>
> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

Cloud Computing

Cloud computing is an umbrella term that covers several concepts. Within the scope of legal technology, it most often refers to Software-As-A-Service ("SaaS"). There are a ridiculous number of definitions of SaaS, but I think this one sums it up succinctly without using 15 more acronyms requiring definitions:

> "Generally speaking, it's software that's developed and hosted by the SaaS vendor and which the end user customer accesses over the Internet. Unlike traditional packaged applications that users install on their computers or servers, the SaaS vendor owns the software and runs it on computers in its data center. The customer does not own the software but effectively rents it, usually for a monthly fee. SaaS is sometimes also known as hosted software or by its more marketing-friendly cousin, 'on-demand.'"

To be clear, this means that you do not have the software installed on your computer - it is accessible only via a browser on the Internet. Further, your data and/or documents are located on the vendor's servers and not on your computer or server.

This obviously raises ethical concerns because you are entrusting client confidential information with someone other than you and your employees.

An excellent compilation of ethics decisions around the country can be found at the ABA Law Practice Management Section's Legal Technology Resource Center (LTRC).

http://www.americanbar.org/groups/departments_offices/legal_technology_resources.html

Probably the best decision that I have read to date in the U.S. comes from Pennsylvania:

http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/saas.html

Pennsylvania, and nearly every jurisdiction who has addressed the issue employ a standard of reasonableness and typically requires segregation of data, privacy/security of data, ability to keep a local download, and reliability of the vendor. The court stated:

The standard of reasonable care for "cloud computing" may include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;

- Installing a firewall to limit access to the firm's network;
- Limiting information that is provided to others to what is required, needed, or requested;
- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the lawyer provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;
- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;
- Ensuring the provider:
    - explicitly agrees that it has no ownership or security interest in the data;
    - has an enforceable obligation to preserve security;
    - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
    - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
    - includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled;
    - provides the firm with right to audit the provider's security procedures and to obtain copies of any security audits performed;

- will host the firm's data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania;

- provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,

- provides the ability for the law firm to get data "off" of the vendor's or third-party data hosting company's servers for the firm's own use or in-house backup offline

- Investigating the provider's:

  - security measures, policies and recovery methods;

  - system for backing up data;

  - security of data centers and whether the storage is in multiple centers;

  - safeguards against disasters, including different server locations;

  - history, including how long the provider has been in business;

  - funding and stability;

  - policies for data retrieval upon termination of the relationship and any related charges; and,

  - process to comply with data that is subject to a litigation hold.

- Determining whether:

  - data is in non-proprietary format;

  - the Service Level Agreement clearly states that the lawyer owns the data;

  - there is a 3rd party audit of security; and,

  - there is an uptime guarantee and whether failure results in service credits.

- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.

- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

In Oregon, while the model rule language in Comments 18 & 19 has not been explicitly adopted, in Formal Opinion No. 2011-188 (revised 2015) they have adopted "the rule to act reasonably" as it applies to an lawyer's obligation under Rule 1.6 to protect client confidential information. Opinion 2011-188 specifically concludes that a lawyer may contract with a third-party vendor to store and retrieve files online via the Internet (i.e., cloud computing).

In Canada, only the Law Society of British Columbia has directly addressed cloud computing, and the Legal Education Society of Alberta has adopted the same standard. It seems to be a higher standard than the U.S., and many practicing in other areas of Canada that haven't addressed it have felt comfortable following the U.S. rules. The Law Society of BC developed an extensive checklist that is submitted as a separate paper hereto. The checklist encourages potential cloud service users to consider, among other things:

- use of a private cloud, which is designed to offer the same features and benefits of public cloud systems without some of the typical cloud computing concerns such as data control, security, and regulatory compliance;
- encryption of data using a 3rd party encryption product and the compatibility of the 3rd party product with the cloud provider's product and services;
- data security and responsibility for specific aspects of security, including firewall, encryption, password protection and physical security;
- regulatory requirements, including statutory privacy requirements, retention periods indicated in the LSBC Rules, the ability to produce documents with respect to a LSBC investigation in the form and time prescribed, and the retention of custody over client data;
- adequacy of remedies in the event of data breaches, data loss, indemnification obligations, and service availability failures;
- the cloud provider's breach notification obligations;
- termination of the services agreement with the cloud provider, specifically as it relates to issues including cost, service level failures (bandwidth, reliability, etc.), data availability after termination, and transition services;

- technical considerations, including compatibility with existing systems, uptime, redundancies, bandwidth requirements, security measures, and technical support service availability; and
- the track record of the cloud services provider (such as uptime, security, support service level, etc).

The above is neither an exhaustive list of applicable considerations nor a complete summary of the Checklist.

Advantages of Cloud Computing (Saas):

- Up Front Price Advantage: Let's say you want to start using a case management application for your practice. If you were to buy one such as Time Matters, you would have to pay for the software outright along with the annual maintenance contract which is mandatory ($905 for the first license and $525 for each license thereafter). You may have to buy a file server or otherwise upgrade your hardware in order to run the program. For an example cost, a new server plus installation and setup could easily run $5,000 - $8,000. Therefore, buying software may turn out to be quite expensive. In the alternative, you would begin subscribing to something like www.rocketmatter.com in which case you would pay $59.99 for the first user per month and $49.99 per user for the next 5 users per month. You wouldn't have to buy a server and you probably wouldn't have to upgrade any of your existing equipment assuming you already have high speed Internet access.

- Ease of Use

- World-Class Data Security

- New Hardware often NOT Required: If you already have a computer and high speed Internet access, then you probably don't need anything else from a hardware perspective.

- Works in Apple or Windows: Since these applications are browser based, they will usually work with both Apple and Windows computers.

- Updates Included: Most cloud application include all updates which are installed for you.

- Technical Support Included: With most cloud applications, you get "free" technical support included with your monthly subscription fee. Of course, purchased software also provides technical support but it is often an extra fee on top of the original software purchase price.

- Access From Anywhere: As long as you're using a computer with internet access, you can probably use your cloud applications. You wouldn't need a VPN, GotoMyPc, or any other type of additional remote access application to accomplish this.

- Share Applications Among Users Spread Out Geographically: For lawyers with multiple offices or who wish to work from multiple locations, cloud applications provide a lot of flexibility. Of course, there are other ways to gain access to programs besides subscribing to cloud applications, but this feature is obviously built in to cloud apps without buying anything else.

- Redundancy Provided: Since your data is stored on the host company's servers, they almost always provide redundant data storage along with that so that there is little (if any) risk that you would lose your data or access to your application due to a physical hardware failure.

E-Mail Encryption and Other Pitfalls

❶ To Encrypt or Not to Encrypt?

According to most jurisdictions in the United States, a lawyer does not violate the duty to preserve confidences and secrets if an email is sent without encryption technology.

In Canada, the rules do not explicitly say that encryption is not required. Instead, the rules imply a duty to act reasonably to protect client confidences. Lawyers should consider the use of information technologies to communicate with the client in a timely and effective manner appropriate to the abilities and expectations of the client. Lawyers may use email (see Rule 3.1-1(d) and 3.1-2 of the Rules of Professional Conduct).

Lawyers must display the same care and concern for confidential matters regardless of the information technology being used. When communicating confidential information to or about a client, lawyers should employ reasonably appropriate means to minimize the risk of disclosure or interception of data by malicious intruders.

What are the risks that a particular information technology poses for inadvertent disclosure or interception? Lawyers should inform a client of the risks of unauthorized disclosure and interception before using information technologies. Lawyers need to ensure that their clients, too, understand that they need to protect the confidentiality of communications to them. Seeking client consent before using a particular technology for communications may be appropriate.

In Ohio, Ethics Opinion 99-2, issued April 9, 1999, by contrast states that a lawyer does not violate the duty to preserve confidences and secrets if an email is sent without encryption technology citing DR 4-101 of the Ohio Code of Professional Responsibility. A lawyer must use his or her professional judgment in choosing the appropriate method of each attorney-client communication. Most jurisdictions in the U.S. are consistent with Ohio.[1] Also see Formal Opinion No. 99-413 of the American Bar Association

---

[1] Excerpt from Ohio Op. 99-2:

The trend among advisory bodies in other states (and the District of Columbia) is that electronic mail without **encryption** is ethically proper under most circumstances.

In the District of Columbia, "[i]n most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security." District of Columbia Bar, Op. 281 (1998).

In Illinois, "[l]awyers may use electronic mail services, including the Internet, without **encryption** to communicate with clients unless unusual circumstances require enhanced security measures." Illinois State Bar Ass'n, Op. 96-10 (1997).

In New York, the state bar association advised that "lawyers may in ordinary circumstances utilize unencrypted Internet **e-mail** to transmit confidential information without breaching their duties of confidentiality under Canon 4 to their clients, as the technology is in use today. Despite this general conclusion, lawyers must always act reasonably in choosing to use **e-mail** for confidential communications, as with any other means of communication. Thus, in circumstances in which a lawyer is on notice for a specific reason that a particular **e-mail** transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet **e-mail**." New York State Bar Ass'n, Op. 709 (1998). The city bar association advised that "[a] law firm need not **encrypt** all **e-mail** communications containing confidential client information, but should advise its clients and prospective clients communicating with the firm by **e-mail** that security of communications over the Internet is not as secure as other forms of communication." Ass'n of the Bar of the City of New York, Formal Op. 1998-2 (1998).

In North Dakota, "Rule 1.6 of the North Dakota Rules of Professional Conduct is not violated by a lawyer who communicates routine matters with clients, and/or other lawyers jointly representing clients, via unencrypted electronic mail (**e-mail**) transmitted over commercial services (such as America Online or MCI Mail) or the Internet unless unusual circumstances require enhanced security measures." State Bar Ass'n of North Dakota, Op. 97-09 (1997).

In Vermont, "[a] lawyer does not violate DR 4-101 by communicating with a client by **e-mail**, including the Internet, without **encryption**." Vermont Bar Ass'n, Op. 97-5.

One state is reticent in its advice regarding unencrypted electronic communication with clients. In Arizona, the state bar responded "Maybe" to the question "Should lawyers communicate with existing clients, via **e-mail**, about confidential matters?" They advised "it is not unethical to communicate with a client via **e-mail** even if the **e-mail** is not **encrypted**" but suggested "it is preferable to protect the attorney/client communications to the extent it is practical." The committee suggested using a password known only to the lawyer or client, using **encryption** software, or at a minimum using a cautionary statement such as "confidential" and "Attorney/Client Privileged" either in the "re" line or beginning the communication. An additional suggestion was to caution clients about transmitting highly sensitive information via **e-mail** if the **e-mail** is not **encrypted** or otherwise secure from unwanted interception. Attorneys were "reminded that **e- mail** records may be discoverable." State Bar of Arizona, Op. 97-04 (1997).

Several states have reconsidered their initial views on the issue. In South Carolina, the bar association first advised that "unless certainty can be obtained regarding the confidentiality of communications via electronic media, that representation of a client, or communication with a client, via electronic media, may violate Rule 1.6, absent an express waiver by the client." South Carolina Bar, Op. 94-27 (1995). Later, the bar advised that "[t]here [now] exists a reasonable expectation of privacy when sending confidential information through electronic mail (whether direct link, commercial service, or Internet). Use of electronic mail will not affect the confidentiality of client communications under South Carolina Rule of Professional Conduct 1.6." South Carolina Bar, Op. 97-08 (1997).

In Iowa, the bar association rescinded Formal Op. 95-30 and replaced it with Formal Op. 96-1 advising that "with sensitive material to be transmitted on **E-mail** counsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgment includes consent for the communication thereof on the Internet or non-secure Intranet or other forms of proprietary networks, or it must be **encrypted** or protected by password/firewall or other generally accepted equivalent security system." Iowa State Bar Ass'n, Op. 96-1 (1996). See also Iowa State Bar Ass'n Op. 96-33 (1997). Later, the bar

Standing Committee on Ethics and Professional Responsibility, *Protecting the Confidentiality of Unencrypted Email*, dated March 10, 1999.

The opinion contains an important caveat that should not be ignored:

> The conclusions reached in this opinion do not diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated media of communication. Particularly strong protection measures are warranted to guard against the disclosure of highly sensitive matters. Those measures might include the avoidance of e-mail, just as they would warrant the avoidance of the telephone, fax and mail.

Is there a problem with this decision that is was issued so long ago? What effect do the newer Model Rules have on this opinion? Despite advances in technology, and the rules in most jurisdictions, the opinion would stand up today.

First, the same opinion is shared in well over a majority of jurisdictions, many of which had the New Model Rules already in place. Comment 17 to Rule 1.6 states:

> [17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. **Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.** A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

The ABA accepted the same approach in Comment 16 to Model Rule 1.6.

---

association amended Opinions 96-1 and 96-33 by advising that "with sensitive material to be transmitted on **e-mail** counsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgement includes consent for communication thereof on the Internet or non- secure Intranet or other forms of proprietary networks to be protected as agreed between counsel and client." Iowa Bar Ass'n, Op. 97-1 (1997).

Second, email is a very efficient form of communication. Third, the same security issues exist in other forms of communication such as wiretapping phone lines or stealing U.S. mail. Fourth, any interception of email or older forms of communication such as US mail or telephone calls is illegal. Finally, there is support in case law for the proposition that a reasonable expectation of privacy may exist even though a form of communication is capable of being intercepted, citing *State v. Bidnost*, 71 Ohio St. 3d 449, 461 (1994).

Ohio accepted the same approach in Comment 19 to its rule 1.6:

[19] When transmitting a communication that includes information relating to the representation of a client, **the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients**. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. **A client may require the lawyer to implement special security measures not required by this Rule** or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Duty to Do More? … Some Say Yes

Pennsylvania and New Jersey have adopted the same rule, but added a little more stringency to it. In Pennsylvania, Informal Opinion 97-130, issued September 26, 1997, concluded:

1. A lawyer may use e-mail to communicate with or about a client without encryption;
2. A lawyer should advise a client concerning the risks associated with the use of e-mail and obtain the client's consent either orally or in writing;
3. A lawyer should not use unencrypted e-mail to communicate information concerning the representation, the interception of which would be damaging to the client, absent the client's consent after consultation;
4. A lawyer may, but is not required to, place a notice on client e-mail warning that it is a privileged and confidential communication; and,
5. If the e-mail is about the lawyer or the lawyer's services and is intended to solicit new clients, it is lawyer advertising similar to targeted, direct mail and is subject to the same restrictions under the Rules of Professional Conduct.

While other jurisdictions are not bound by rules 1 through 5, above, I recommend them as best practices to follow.

The New Jersey Advisory Committee on Professional Ethics, in Opinion 701, issued in April 2006, states in a footnote that confidential documents sent over the Internet should be password protected.

In conclusion, in light of evolving technology and rules, it is my recommendation that lawyers (1) should advise clients verbally and in their engagement letter about email, as described in the Pennsylvania opinion, and (2) should have encryption available for use in appropriate circumstances.

❷ Email Encryption Solutions

Office 365 w/hosted Exchange and E3 licensing
www.office.com

Protected Trust
www.protectedtrust.com

Mail It Safe
www.mailitsafe.com

AppRiver
http://www.appriver.com/services/email-encryption/

Send
www.sendinc.com

TrendMicro
http://www.trendmicro.com/us/enterprise/network-web-messaging-security/email-encryption/index.html

❸ Retracting Sent E-Mails

Are there times when you wish that you could UNSEND something? This is actually something that can be done to prevent a known ethical violation where it may not be possible with ordinary U.S. Mail. With U.S. Mail, once the mail is in the post box, good luck getting it back!

I have 2 suggestions in this regard:

- If your firm uses Exchange Server, be sure to tell your system administrator to set a 5 minute delay before the email is actually sent from your server. This may give a user in your office enough time to catch it before it goes out.

- You may want to try out something like www.mailitsafe.com, or similar functioning service, which is an email verification program, but also allows retraction so long as it hasn't been retrieved by the recipient. You can also encrypt emails and attachments, requiring recipients to use passwords to open. The cost is $150 per year.

❹ E-Mail Addressing: AutoComplete can be an AutoDisaster

Outlook and other popular email programs have an ”Auto-Complete” function that saves you the time of having to type out someone’s complete email address if the name already exists in the program’s address book. Once you type the first character in the TO field, Outlook starts guessing the name of the recipient and will display potential names. If to quick and careless, you could accidentally hit ENTER and auto-complete the wrong recipient. While a nifty feature if used correctly, this can get you into trouble if you are careless.

As an example, if you intend to send something to your client “Brian Cluxton”, you could accidentally send something to opposing counsel “Brian Clayton” by typing B-R-I and hitting ENTER too quickly. If you don’t catch it, you could send something really damaging to the wrong person. I don’t think this warrants disabling the feature … just be careful!

Metadata Pitfall

You just hit the SEND button. You start to sweat and suddenly experience a panic attack. You and your associate were revising a contract for a client. Before sending it on to your client, you forgot to accept or reject tracked changes and remove all the hidden text from the word processing document. You also forgot to remove any other "metadata" before sending it. Anyone who receives the file can easily find out the following information:

- All the people who authored any part of the document … including the original author who happens to be a managing partner at a competing law firm
- The hidden text that states the client "is a moron!"
- The suggested changes made by a 1st year associate in your office (half of which were a bit moronic)
- The total time you spent revising the document … 15 minutes (even though you billed the client 8 hours – which is a big ethical problem of its own!)

This story is not fictional. It actually happened. This is just one of many bad messes that you can get yourself into if you are not using technology correctly.

The Bad News … Say goodbye to the glory days when you could simply draft and send a word processing document to opposing counsel or your client.

The Good News … Most technology-created pitfalls are easily avoidable if reasonable steps are taken.

Metadata … Is it really a "Nightmare"?

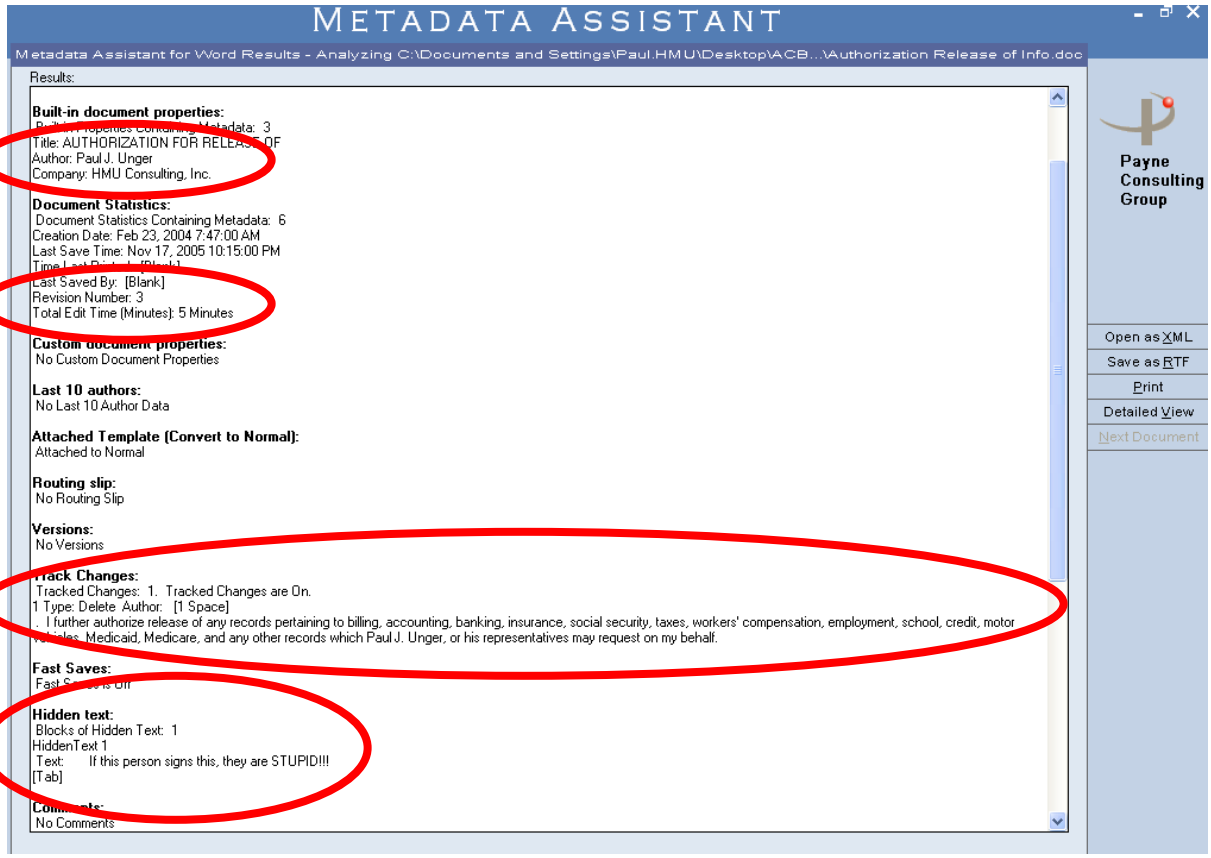
What is Metadata? Literally, metadata means "data about data." In the personal & business computing world, it is the hidden or invisible information contained within computer files. Most notably in the legal technology field, lawyers worry about metadata found in Microsoft Word, PowerPoint, Excel, Corel WordPerfect and Adobe Acrobat files.

The kind of information that can be found under the surface a Word document, for example, might be:

- Last 10 authors
- Firm name
- File locations

- Tracked changes
- Hidden text
- Deleted document comments
- Routing slip information
- Document versions
- Revision time
- Document properties (file size, modification date, etc.)
- Fast saves
- Hyperlinks
- Linked objects

As an example, below is part of a report showing metadata using a widely-used metadata remover called "Metadata Assistant" created Payne Consulting Group.



Why have metadata if it is so bad? Well, quite frankly because it is really useful information and it was never intended to be bad. Microsoft designed its programs to store metadata for a variety of reasons, one of which was for document management before Document Management Systems (DMS) existed.

As a very simple example, if one wanted to find all documents created or modified between December 1, 2005 and December 31, 2005 as a way to verify that you created

timesheets for all your billable time in December, you would perform a search using a Microsoft Find Files or Folders utility or a third-party program like dtSearch that searches … yes … metadata.

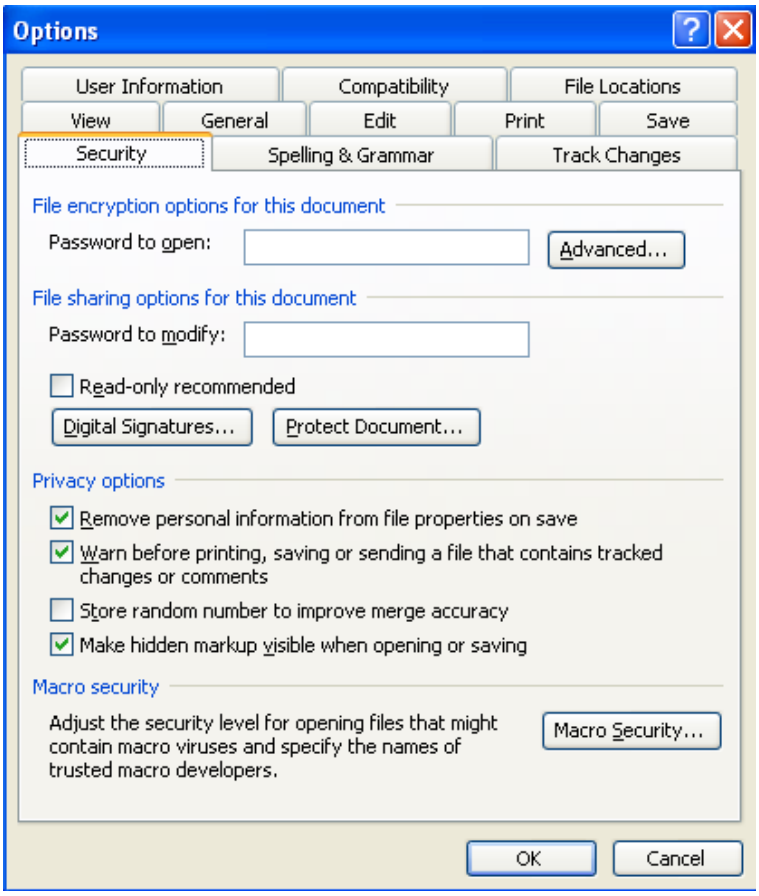
If you exchange electronic word processing files with anyone outside your office and do nothing to remove metadata it can result in a nightmare if the file contains metadata that was intended to be confidential. So, yes, it can indeed be a nightmare as many legal technologists claim. However, if you are not careless, these problems are not a nightmare at all. You just need to know what to do. Below is a list of what you need to do to avoid the word processing so-called "metadata nightmare."

❶ Learn the Security Settings within Microsoft Word

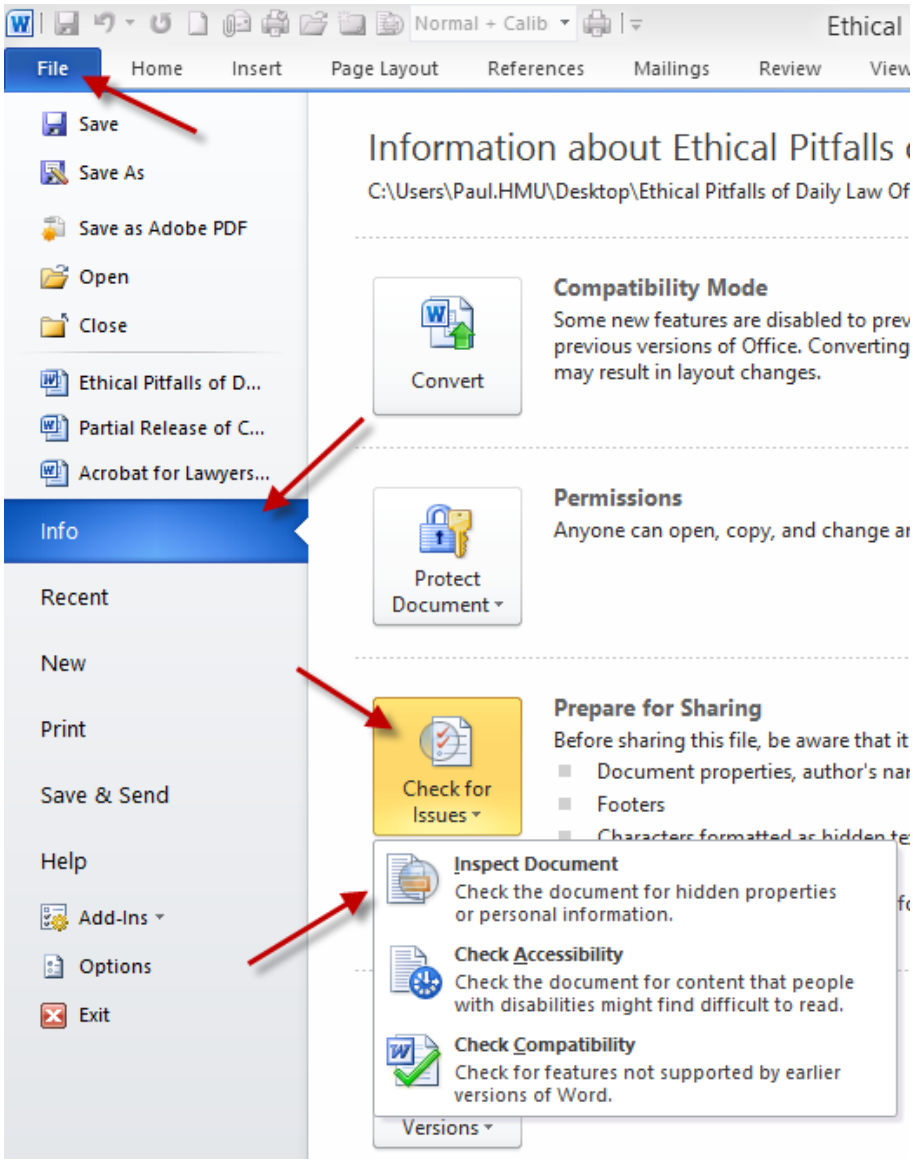
Much of the "dangerous" metadata contained in Microsoft Word documents can be prevented from transmission if certain security features are turned on.

In Word 2003 and earlier, open Word and select **Tools** and then **Options** and select the **Security** tab:

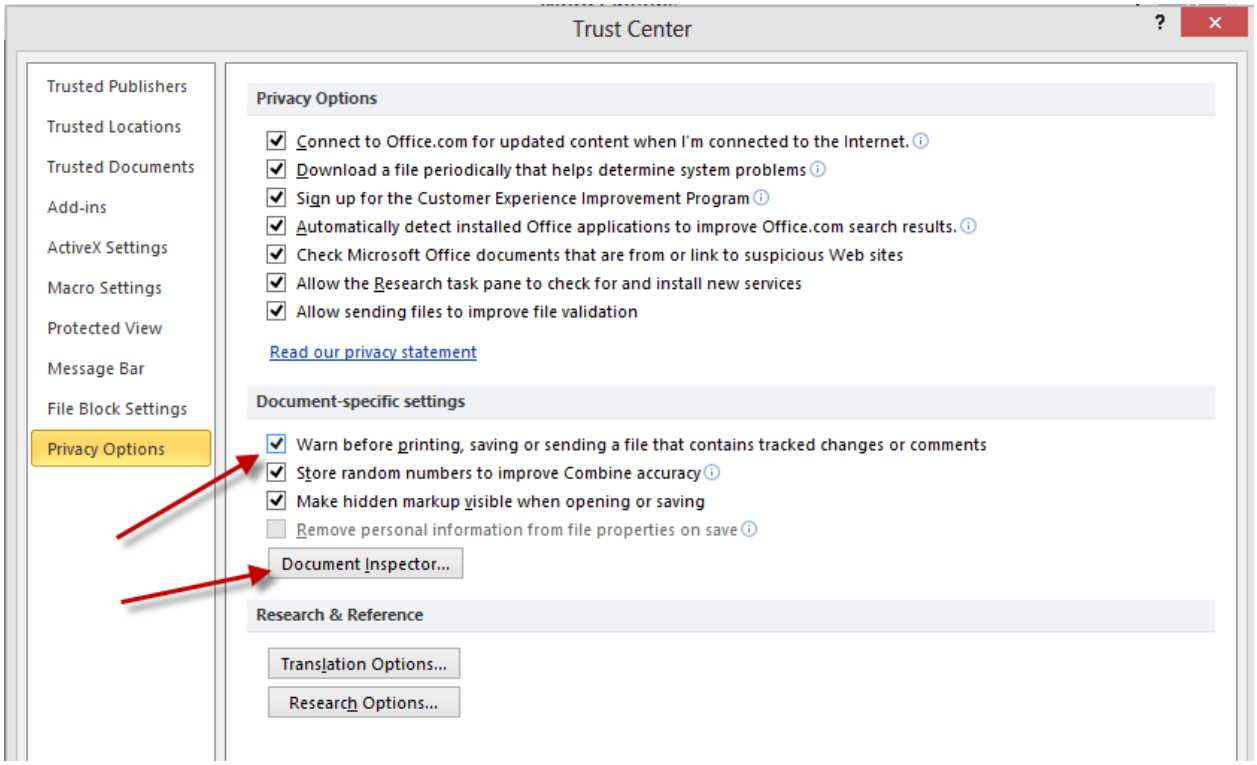
- Check "Remove personal information from file properties on save"
- Check "Warn before printing, saving or sending a file that contains tracked changes or comments"
- Check "Make hidden markup visible when opening or saving"



In Word 2010 and later, you must run the document inspector, which is most easiest found at **File > Info > Check for Issues > Document Inspector.**


Normal + Calib
Ethical
File
Home
Insert
Page Layout
References
Mailings
Review
View
Save
Save As
Save as Adobe PDF
Open
Close
Ethical Pitfalls of D...
Partial Release of C...
Acrobat for Lawyers...
Info
Recent
New
Print
Save & Send
Help
Add-Ins
Options
Exit
Information about Ethical Pitfalls
C:\Users\Paul.HMU\Desktop\Ethical Pitfalls of Daily Law Of
Convert
Compatibility Mode
Some new features are disabled to prev
previous versions of Office. Converting
may result in layout changes.
Protect Document
Permissions
Anyone can open, copy, and change ar
Check for Issues
Prepare for Sharing
Before sharing this file, be aware that it
Document properties, author's nar
Footers
Inspect Document
Check the document for hidden properties or personal information.
Check Accessibility
Check the document for content that people with disabilities might find difficult to read.
Check Compatibility
Check for features not supported by earlier versions of Word.
Versions

You may want to have Word warn you if there are tracked changes comments on save, print or send commands. It is found under **File** and then **Options**, **Trust Center, Trust Center Settings**, and then **Privacy Settings**.



You can also download and install a free add-in from Microsoft - Office 2003/XP Add-in: Remove Hidden Data. CAUTION: This will not remove all metadata. Metadata still exists. The question is whether it is benign or damaging metadata.

❷ Learn About Tracked Changes in Word

"Track Changes" is a fantastic feature available in Microsoft Word that allows multiple reviewers of a document to literally track changes or compare documents electronically to see what edits have been made to a document. My first suggestion is to start using it if you have the need for that type of feature. My second suggestion is to learn how to use it correctly so those internally tracked changes do not end up in the hands of opposing counsel or even your own client. Here is an example of a paragraph that has tracked changed turned on.

"Track Changes" is a fantastic feature available in Microsoft Word that allows multiple reviewers of a document to literally track changes or compare documents electronically to see what edits have been made to a document. My first suggestion is to start using it if you have the need for that type of feature. My second suggestion is to learn how to use it correctly so those internally tracked changes do not end up in the hands of opposing counsel or even your own client so you don't look like a freaking idiot. ~~Here is an example of a paragraph that has tracked changed turned on.~~

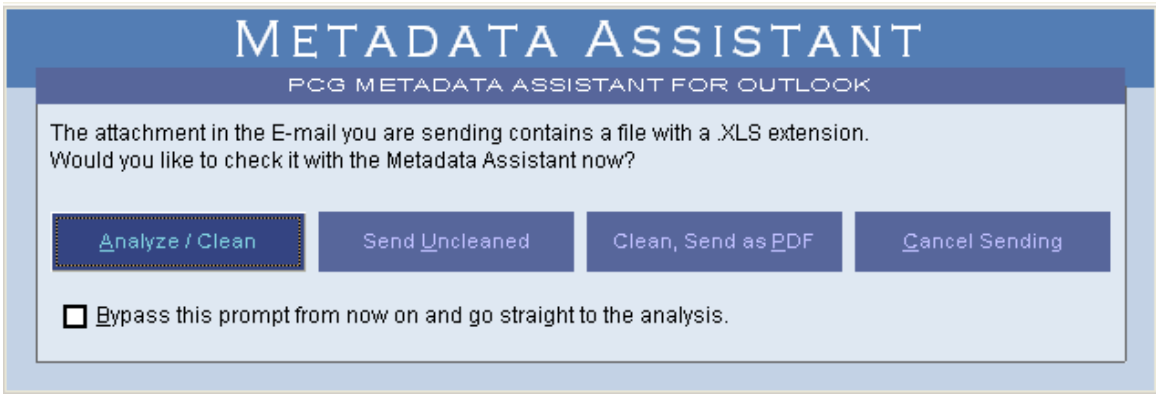
Added Text & Deleted Text

The first big mistake that people make is not accepting or rejecting all changes before sending the document on to opposing counsel for their review. It is imperative that you go through the entire document and accept or reject all the changes made in the document. Changes that were made between versions that are not **accepted** or **rejected** will show up in a metadata analysis. This may expose your thought process or a weakness that you knew about, but the other side didn't think of … at least until now!

The second critical thing that you do is make sure that you can see the tracked changes (the marked up or redlined version). Be sure that you select **Final Showing Markup** in the reviewing toolbar. Otherwise, you may not even realize that there are tracked changes in the document. Also remember in the security settings (discussed above) there is an option that will warn you before printing, saving or sending a document that has tracked changes.

❸ Consider a Third-Party Meta Data Removal Tool

Another option which I generally favor is investing in a metadata removal tool. These are programs that strip the metadata out of electronic documents before you send it to another party. You can either run the cleaner manually on a document OR intercept, evaluate and clean all attached documents when you are emailing it to the outside world. This makes the process much easier and requires no working knowledge of how tracked changes work or security settings within the program. As an example, Donna Payne's Metadata Assistant intercepts attachments with this dialog box when you hit the **Send** key from Outlook's email:



I suggest a metadata remover for those people who actually exchange electronic documents containing potentially harmful metadata. Many lawyers don't do this. If you do not exchange documents, don't spend the money.

Metadata removal tools to consider:

- Metadata Assistant (Payne Consulting Group – www.payneconsulting.com). Cost is $79 per license.
- CleanDocs (www.cleandocs.com)
- Workshare Protect (www.workshare.com). Cost is $29.95 per year.
- iScrub by Esquire Innovations (www.esqinc.com).
- Out-of-Sight by SoftWise (www.softwise.net). Cost is $30 per user.
- ezClean by KKL Software (www.kklsoftware.com). You must buy at least 20 licenses at $20 per license.

❹ Exchange PDF Documents

Although PDF documents do contain some metadata, they do not contain as much. Tracked changes can indeed be passed on from a Word document to PDF, but you would have to do it one of two ways. First, the person converting the document would have to attach the Word file into the PDF in its native format (Acrobat allows you to attach files into a PDF document). While possible, I know of no one who uses that function. So…just don't do it that way. A second way is if you have the tracked changes visible when you convert to PDF. That would create a PDF with the tracked changes blatantly showing. You would have to be blind or extremely careless not to see the tracked changes in the Word document and the resulting PDF. Also, if you have your printing configuration in Word set to print 'tracked changes' along with the document. In this instance, again, you would have to be blind and 100% careless by failing to review the newly created PDF before sending it.

Another benefit sending a PDF is that PDF documents are less editable, especially if you have security turned on. This has less to do with metadata, but it is a nice benefit if you send a PDF to a client, for instance, and tell them to print and sign the attached. If the document is editable, the client could change the text using Adobe Acrobat and then sign it (and not tell you). If the PDF document is secure, the signing party would have to go to greater lengths to make a deceptive change that is not noticeable.

❺ WordPerfect also contains Meta Data

Contrary to popular belief, WordPerfect also contains metadata. Examples of metadata stored in WordPerfect documents include:

- Authors
- Tracked changes
- Comments and hidden text
- Document revision annotations
- Undo/Redo history
- User names, initials and company
- Document summary information
- Header/Footer information
- Hyperlinks

See Minimizing Metadata in WordPerfect 12 Documents, Corel Corporation, copyright 2004.

Like Microsoft, Corel also made available a metadata removal tool which is available on their website. Also check WordPerfect Universe (www.wpuniverse) which offers a metadata removal tool for WordPerfect.

Keeping Information Safe from Disaster, Accidental Loss, Theft, Viruses and Malicious Intruders

ABA Model Rule 1.6 also imposes a duty upon lawyer to keep their technology in safe and working order to protect client information. Similarly, in Canada, Section 3.3 of the Rules of Professional Conduct requires competence and confidentiality.

As an example, section 5.7 of the Law Society of Upper Canada's Technology Practice Management Guidelines states:

5.7 Confidentiality

Lawyers using electronic means of communications shall ensure that they comply with the legal requirements of confidentiality or privilege. (Section 3.3 of the Rules of Professional Conduct).

When using electronic means to communicate in confidence with clients or to transmit confidential messages regarding a client, a lawyer should

- develop and maintain an awareness of how to minimize the risks of disclosure, discovery or interception of such communications
- discuss the inherent security risks associated with each technology with the client and confirm in writing that the client wishes to communicate using that method
- use firewalls and security software to protect at-risk electronic information
- use and advise clients to use encryption software to assist in maintaining confidentiality and privilege
- take appropriate measures to secure confidential information when using cloud-based services
- develop and maintain law office management practices that offer reasonable protection against inadvertent discovery or disclosure of electronically transmitted confidential messages.

ABA Model Rule 1.6(a) states:

> (a) A lawyer shall not reveal information relating to the representation of a client, including information protected by the attorney-client privilege under applicable law, unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by division (b) or required by division (c) of this rule.

Comment 16 further states:

> Acting Competently to Preserve Confidentiality [16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3.

The State Bar of Arizona issued an opinion in response to an inquiry about the steps a law firm must take to safeguard data from hackers and viruses. They stated:

> ER's 1.6 and 1.1 require that an attorney act competently to safeguard client information and confidences. It is not unethical to store such electronic information on computer systems whether or not those same systems are used to connect to the internet. However, to comply with these ethical rules as they relate to the client's electronic files or communications, **an attorney or law firm is obligated to take competent and reasonable steps to as-sure that the client's confidences are not dis-closed to third parties through theft or inadvertence.** In addition, an attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information **is not lost or destroyed.** In order to do that, an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence. (Emphasis added.)

State Bar of Arizona, Opinion No 05-04, July, 2005.

The ABA Standing Committee on Ethics and Professional Responsibility has stated something similarly. In Opinion 95-398, they concluded "[a] lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of the client information."

In 2006, Nevada spoke to a similar issue relating to offsite storage of data and reached a consistent conclusion. They stated that a lawyer may store confidential information electronically with a third party to the same extent and subject to the same standards as storing confidential paper in a third party warehouse. In doing so, the lawyer must act" competently and reasonably to ensure the confidentiality of the information. Opinion 33 (February 9, 2006), Nevada Standing Commission on Ethics and Professional Responsibility.

David Reis, a partner with Thorp, Reed & Armstrong, LLP in Pittsburgh, PA, and a colleague legal technologist suggests the following basic steps:

1. Keep your operating systems patched.

2. Install and use anti-virus and spyware protection on all computers (and keep them all current with updates).

3. Use Care with Email attachments and Embedded Links.

4. Make backups of important files and folders.

5. Use strong passwords or other authentication (combine numbers and characters).

6. Use care when downloading and installing programs.

7. Install and use a hardware firewall.

8. Install and use a file encryption program.

Additionally, I recommend:

1. Apply the above principles to laptops and PCs that are used at home for business purposes.

2. Have a secondary backup system (consider an online backup service like Iron Mountain, MozyPro or Carbonite).

3. Encrypt laptops and external hard drives or flash drives where you store or transfer client information.

4. Use Adobe Acrobat Pro (or similar competing products like Kofax PowerPDF Advanced, pdfDocs, etc.) to redact important client information (social security numbers, billing information, etc.) contained in documents that you may have to file with the court electronically.

Disposing of Old Computer Equipment

You just got all new workstations for your staff. What do you do with the old workstations? What about all the confidential information contained on the hard drives? If you think that you deleted the information, think again! You may be violating Model Rule 1.6, HIPAA and opening yourself up to liability.

According to a study performed at the Massachusetts Institute of Technology (MIT), two graduate students scavenged through the data inadvertently left on 158 used disk drives. They found more than 5,000 credit card numbers, detailed personal and corporate financial records, numerous medical records, gigabytes of personal email and pornography. The disk drives were purchased for less than $1,000 from eBay and other sources of used computer hardware. Only 12 were properly sanitized (http://web.mit.edu/newsoffice/2003/diskdrives.html) .

❶ Avoiding the Ethical Pitfall – What is Required?

A lawyer must act reasonably to preserve confidences and secrets of his/her client. The rules in the U.S. and Canada impose the same duty. ABA Rule 1.6 (and old rule DR 4-101) imposes a duty to preserve confidences and secrets. In all likelihood, disposing of employee workstations was not contemplated when DR 4-101 was adopted by the Supreme Court of Ohio on October 5, 1970 and likewise in other jurisdiction following suit; nevertheless, the rule applies. The New Rule as written, establishes a broad duty to preserve confidences and secrets that applies to all methods of communication. The duty clearly extends to disposing of client information and communication.

What does this mean in practical terms? Reasonableness, in my opinion, requires one of the following:

(A) Retain the hard drive(s) of the computer(s) for safe keeping; or
(B) Hire a company to erase and reformat the hard drives[2]; or
(C) Hire a company that uses a special data erasing program.

[2] Erasing and reformatting hard drives will not completely protect the data. A skilled computer technician or forensic expert can likely recover some (not all) data from that hard drive using specialized software. This process is time-consuming and expensive.

❷ Use a Computer/Electronics Recycling Service

Seek out a reputable computer disposal vendor in your area. In Canada and U.S., and depending on your location, Global E Waste Solutions (www.globalewaste.net) offers these services, as well as Iron Mountain (www.ironmountain.com). Both companies are reputable vendors who are committed to proper data destruction and not filling up landfills with electronics.

In the U.S., PCDisposal, IT AMG Disposal Services, and Retire-IT offer these services nationwide. They will pick up your units (or have them shipped), properly delete data, and provide a certified report.

PCDisposal.com
Toll Free: 877-244-0250
www.pcdisposal.com

I.T. AMG Disposal Services
Toll Free: 877-625-4872
www.itmag.com

Retire-IT
Toll Free: 888-839-6555
www.retire-it.com

Local Vendors: Similarly, there may be numerous local vendors in your area who provide these services if you prefer to support local businesses. A quick Google search will identify potential candidates.

Get Multiple Quotes: This is a competitive business so it is to your benefit to obtain quotes from more than one vendor!

IMPORTANT: Many computer recycling companies will not sanitize data. Make sure that you specifically request this, or it may not be done.

❸ Do-It-Yourself

You could do the DOD-level data destruction yourself with programs like the ones listed below, OR simply take out your screwdriver and physically remove the hard drive and throw it in a locked file cabinet. Programs that you can buy to erase data yourself are:

- cyberCide Data Destruction (www.cyberscrub.com) offers a product for $29.00.
- Active@ Kill Disk - Hard Drive Eraser (www.killdisk.com/eraser.htm) offers a free version and a professional version for about $30.
- OnTrack DataEraser™ (www.ontrack.com) offers a personal version for $29.

IMPORTANT NOTE: If trying to **sanitize data on a solid state drive (SSD)** (most hard drives after 2013), I recommend that you use Parted Magic (www.partedmagic.com), or rely on an expert to do it for you and provide written certification. The above tools will not work on SSDs.

❹ Don't Forget SmartPhones, Tablets, and Copy Machines!!

Be sure to follow manufacturer's instructions on wiping all data from smartphones and tablets.

Copy machines are the most often forgotten about devices that contain an enormous amount of potentially confidential client information. Copy machines just don't copy anymore. They first take a snapshot image of the document, stores it on a hard drive, and then prints a copy per your instructions. Depending on the size of the hard drive and the volume you scan, your machine can hold days, weeks, months, and potentially years of "copied" documents.

CBS did an excellent story on copy machines that is quite alarming:
http://www.youtube.com/watch?v=iC38D5am7go

Password Management and Two-Factor Authentication

In short, passwords need to be (1) unique; (2) strong; and (3) stored safely. With as many passwords that we maintain, personally and professionally, there are some very inexpensive, but fantastic solutions that can provide you with relief.

❶ Two-Factor Authentication is Critical

Putting in place two-factor (or multi-factor) authentication (also known as 2FA) is more important today than changing passwords or using unique passwords. I still think unique passwords is important, but changing passwords every 30 days has recently been regarded as a waste of time. 2FA is more important because without the second method of authentication (usually a text message notification requiring your intervention, like entering a code, providing a PIN, proving your fingerprint from your smartphone) a cybercriminal will not be able to login to an important account even if they have your password. See this regarding Microsoft finally acknowledging this year that 2FA is critical and changing passwords is not very important anymore: https://www.cnet.com/news/microsoft-admits-expiring-password-rules-are-useless/.

❷ Make Passwords Strong and Unique

Passwords should not be re-used. If your credentials are compromised, they could be sold on the dark web. If you used the same password at another site (i.e. Dropbox, a client portal, your bank, etc.) your information (potential confidential information or documents) is now compromised. Moreover, most cybersecurity experts now advise people to use long phrases that combine letters, numbers and characters. I generally aim for at least 12 characters.

❸ Safely Store your Passwords

If you don't have a password manager, I recommend saving your passwords in an encrypted Word or Excel file (see above how to encrypt Word & Excel files).

❹ Password Management Programs

I strongly recommend investing in a password manager. In fact, I believe in this technology so much, that our company now provides a password manager to every employee in our organization. The good news is that the above 3 objectives can be

achieved with some very inexpensive solutions. Here are some of the common features:

- Automatic password generators for unique passwords that never repeat
- Automatic password generators that create insanely strong & cryptic passwords
- Cloud encrypted storage of passwords
- Access to passwords from all mobile and desktop devices
- Integration with all major browsers
- Works on a Mac or PC
- Apps for iPhone, Android-based phones, iPads, Android tablets
- Safe storage of financial and estate information
- Ability to share with loved ones or individuals at work

Highly Rated Password Managers

1. **Dashlane** (www.Dashlane.com)
2. **LastPass** (www.LastPass.com)
3. **1Password** (www.1password.com)
4. **Roboform** (www.roboform.com)
5. **Keeper** (www.keepersecurity.com)

FIGHT the PAPER

HOW TO ELIMINATE PAPER IN THE LEGAL OFFICE

Paul J. Unger | Barron K. Henley

Affinity CONSULTING

FIGHT THE PAPER

How to Eliminate Paper in the Legal Office

Paul J. Unger, Esq. & Barron K. Henley, Esq.
Affinity Consulting Group

MEET THE AUTHORS

PAUL UNGER, ESQ.

Paul J. Unger is a nationally recognized speaker, author and thought-leader in the legal technology industry. He is an attorney and founding principal of Affinity Consulting Group, a nationwide consulting company providing legal technology consulting, continuing legal education, and training. He is the author of dozens legal technology manuals and publications, including recent published books, *How to Effectively Manage your Workload – A Lawyer's Guide to Distraction, Time, Task & Email Management* (2019) and *PowerPoint in an Hour for Lawyers* (2014). He served as Chair of the ABA Legal Technology Resource Center (2012-13, 2013-14)(www.lawtechnology.org/), Chair of ABA TECHSHOW (2011)(www.techshow.com), and currently serves on the Executive Committee for ACLEA (The Association for Continuing Legal Education). Mr. Unger now spends most of his time doing CLE programs, professional development programs for law firms, and conducting technology and practice management assessments.

BARRON HENLEY

Barron is an attorney who has over 22 years of experience in legal technology. After earning his B.S./B.A. (marketing and economics) and J.D. from The Ohio State University, Barron discovered his passion for helping lawyers fix problems within their practice. Today, Barron partners with our clients to make law firms and legal departments more efficient. Barron's breadth of knowledge enables him to dive into the details of a firm's operations. He is often the lead on Comprehensive Practice Analysis projects for clients that examine all aspects of making a firm more successful: technology, organizational design, process optimization and financial practices.

FIGHT THE PAPER
TABLE OF CONTENTS

1 THE PROBLEM WITH PAPER

2 PORTABLE DOCUMENT FORMAT (PDF)

3 SCANNING

4 DUAL MONITORS

5 IPADS/TABLETS

6 SEARCHING YOUR DOCUMENTS

7 DOCUMENT MANAGEMENT SYSTEM

8 DOCUMENT MANAGEMENT WITHOUT DM SOFTWARE (HOME-GROWN DMS)

1 THE PROBLEM WITH PAPER

INTRODUCTION

To achieve effective time, document and email management, we have to "get organized." In order to be organized today, we absolutely must figure out how to manage digital information. According to one study, we receive via digital delivery (email, text, social media, on our phones, computers, etc.), the equivalent of 140 newspapers of information per day! This can be overwhelming, especially if you don't have a system in place to process that digital information.

In most offices today, only 1 attorney in 10 have eliminated 90+% of the paper file. In other words, only 1 in 10 have stopped maintaining a paper file and rely solely on the digital file. While better than nothing, that needs to be significantly better.

The good news is that the tools necessary to eliminate paper are available, easy to use and inexpensive. Of course, this hasn't always been the case. Back in the 90s, scanners were very expensive and relatively slow. Document management systems weren't very easy to use, and they were also expensive and made primarily for large organizations. Electronic storage space on servers was also expensive. Since that time, the tools have steadily improved as their costs have declined. Secure cloud storage is a highly competitive market, and therefore, there are many solutions available at a reasonable cost. As a result, the benefits of paper reduction now far outweigh the costs of implementing such a system.

PROBLEMS WITH PAPER RELIANCE

There is still a heavy reliance on paper for many users in most environments. I realize that some people generally don't see paper reliance as a problem. Therefore, I want to explain why paper reliance represents an efficiency problem and needs to change.

Paper Reliance Means Higher Operating Costs: Most law offices are very interested in ways to save money. Operational efficiency means lower costs and improved profitability. Further, high efficiency and paper reliance are mutually exclusive. Creating paper files, maintaining them, updating them, moving and storing them all require non-billable labor. An organization's number one cost is probably payroll, so paper management factors into that. The paper, toner and office supplies (such as folders) are all expensive. Redweld expanding files are $10 for a 5 pack. Staples copy paper is $46 per case. Avery file labels are $26/pack (Staples); black toner for your copiers and printers is expensive. Further, a percentage of your offices are occupied by filing rooms and filing cabinets. So, you're technically paying rent every month for those files.

The bottom line is that all of these things add up to a large amount of money per year. These costs are a primary reason that courts, banks and almost every business that previously dealt with a lot of paper is now all electronic. Law offices are not exempt from this economic reality.

More Paper Means Limited Mobility: Transporting bulky paper files is difficult and sometimes impossible (depending upon the number one needs). As a result, lawyers often feel tethered to the office because they can't easily take the paper files with them if they need to work remotely.

Too Easy to Lose Something or Drop a Ball: If a lawyer or paralegal has stacks of files and paper all over his/her office, there is no way he/she knows what is at the bottom of those piles. Almost every person I've ever spoken

to who has a big mess of files in their office has claimed "I know where everything is." However, if I pick up a random stack and ask them to tell me everything that's in the pile, they have to admit that they don't know.

Digital Records Are Being Forced on Lawyers: Much of what we do as lawyers, whether we like it or not, is already digital whether we like it or not. ALL documents that we create start out as digital files. They don't start in typewriters! Why do we convert those to paper? Many courts have gone to electronic filing, governmental entities we deal with are electronic, documents are traded between attorneys and clients electronically, and more and more evidence and discovery is electronic. Lawyers who insist on operating with an analog/paper approach will have to keep printing more and more electronic documents in order to maintain a complete paper file. All professional service industries will eventually be electronic because that's the form all of the information they deal with will take. Accountants, physicians, engineers, financial planners and architects are already there. The only question for offices who provide legal services is whether they'll wait until the last minute and be reactive, or get out in front of it proactively.

Overwhelming Volume of Communications to Manage: We machine gun one another with electronic communications resulting in many more pieces of correspondence to keep track of. When I started practicing law 25 years ago, we received an occasional fax and no email. Most correspondence came in the form of letters received via USPS or FedEx. I might have received 3 to 5 pieces of mail a day related to cases I was working on. Today, it's not uncommon for a lawyer to receive 150 emails a day related to their practice, some with attachments and most of which requiring an immediate response. Voice mails are often emailed as sound files and faxes are also often received as emailed PDF files. As a result of this, the volume has exploded and paper-based systems break down as volume increases.

Hunting for Files Is Expensive: All offices who maintain paper case files spend non-billable, administrative time looking for paper files every month. For example, files might be in your office (on the desk, under the desk, on the floor, in a cabinet or on a shelf), in a person's office, on a counter in a hallway, on a ledge somewhere in the office, in a filing cabinet, in the wrong filing cabinet, in someone's car, at someone's home or in someone's briefcase or bag. That's a lot of places to look. The cost associated with finding files can be very high.

Paper Files Can Only Be in One Place at a Time: Generally, only one person can be in possession of a paper file at a time. However, the same electronic files can be accessed by multiple people simultaneously.

Paper Files Are Not Sharable: If you want to share a paper file, then you have no choice but to incur the additional time and expense of making more paper copies. This makes it difficult to collaborate with clients, experts, courts and co-counsel.

Finding the Document Once You've Found the File: Once you locate the paper file, now you begin the second search - finding the individual piece of paper within that file. If the file is really big, it may take just as long to find a document within the file as it took to find the file in the first place.

Paper Files Are Not Searchable: Obviously, you lose the search functionality an electronic file provides.

The Paper File is not Complete and Neither is the Electronic File: Almost everyone I talk with indicates that email is not getting saved into the digital file and some of the work product is not getting saved. Nearly everyone my polls indicate that they feel overwhelmed by email and there isn't an easy way to save incoming and outgoing emails into the digital case file or paper file.

ROADMAP / ESSENTIAL ELEMENTS TO ACHIEVE PAPERLESS

The following are the elements required in every successful paper reduction initiative. The good news is that most organizations have already implemented many of these steps. You may just need to help getting over the finish line with changes in process and some simple training.

Ensure You Have Solid I.T. Infrastructure, Redundant Backup Systems And Security

You must have dependable servers, redundant data backup, and security systems and protocols in place if you are going to eliminate paper. If you implement a cloud-based system, much of this is simplified and solved as part of your monthly service fee. In fact, most reputable cloud providers have achieved and maintain security certifications that would be cost-prohibitive for most organizations. This is another reason most legal departments and law offices are migrating to cloud-based solutions. Within legal departments at corporations or colleges/universities, getting consistent I.T. assistance is tough because of the bureaucratic red tape that is involved and the high turnover of employees within the I.T. department. This makes cloud solutions even more attractive.

Confidence In Your I.T. Department

Unless and until your users have confidence in the people running the system, they will continue to rely on the security of paper. It is their safety blanket.

Acquire Desktop Scanners

This is discussed below, but in short, your staff needs small, fast convenient desktop scanners so they can easily scan documents directly into the digital file right at their desk without having to get up and go stand in line to do their scanning.

Automatic OCR Engine

All PDFs much be searchable, and that process needs to be automatic. You should not use up staff time to run this process. It is too expensive, and it will not get done a great deal of the time, resulting in people believing that documents are searchable, but they are not. See below for discussion on software solutions that can do this for you (Symphony OCR, ndOCR, Content Crawler, etc.).

Document Management System (DMS)

This can be a software solution, or a do-it-on-your-own process by saving documents in a central organized manner within a Windows folder structure. Most experts today agree that the with the volume of email and other digital content that we receive on a day to day basis, that we need software to assist us with document management.

Procedural Requirements

1. **Digitize All Incoming Paper**: Everything that comes in the door must be scanned (excluding advertisements) and then the paper goes in one of three places (preferably #1, below):
    - The shredder
    - Send back to client

- A very thin paper file you may maintain because a statute, regulation or rule requires that you keep the blood-signed original.

2. **Scan Paper Work Product**: For example, lots of lawyers like to write on legal pads. It's perfectly fine to continue doing that as long as the resulting notes are scanned into the electronic file with everything else. Also, think about utilizing tablet-based note taking (I.e., iPad + Notability, Surface Pro + OneNote), and not even having to scan pages torn from legal pads.
3. **All Digital Case Documents must be Stored in DMS or Digital File:** Every PDF, Word document, Excel spreadsheet, PowerPoints, … everything, must be saved to the DMS or digital file and properly categorized based on document type (correspondence, pleadings, agreements, memos, notes, etc.)
4. **Important Case/Matter Email Must Be Stored in DMS or Digital File**: All important email must be stored along with the rest of the electronic documents related to any particular matter. Some important **copies** of emails can still be in Outlook, but copies must be stored in the DMS where the rest of the office can easily access them. Note: One observation that I see people often make is that they to save every email into the digital file, and that just isn't necessary. Saving just the important emails is fine. When people aim for perfection or everything, it paralyzes them, not to mention that it results in time wasted and a ton of redundant emails. Most of the time, with the exception of emails with attachments, the last email in an email conversation contains the entire historical thread.
5. **Workflow Review Method.** There must be a process in place that insures that the intended recipients of the documents, and anyone else, (1) reviews the electronic information, and (2) tasks & deadlines get assigned based on that review. Most offices will have a legal assistant (or a scanning clerk) do the following:
    - scan the document,
    - save it into the proper case/matter,
    - record & assign deadlines,
    - and then forward a **link** to the person that needs to review the document.

Dual Monitors

Dual monitors are absolutely needed for effective paper reduction. I understand that there some may resistance to this idea, but the reality is that dual monitors have not only become standard issue for law offices and legal departments across the country, but this concept is also a key ingredient for helping to reduce reliance on paper. See discussion below on Dual Monitors.

Portable Hardware/Mobility

If every lawyer is tethered to a desktop computer at the office, then the office loses out on a lot of the mobility benefits of being paper-reduced. For lawyers who go to court, meet with clients or work outside of the office, there must be a means for them to take the electronic file with them. Obviously, this is where notebook PCs, tablets or hybrids become very important. Think about adding iPads for some lawyers who are road warriors or who try cases would be extremely valuable.

Conference Room Technology

One reason that lawyers keep paper is to have the file available to them when they go to the conference room to meet with the client. To avoid this evil, you must have presentation technology in the conference room to review file information with the client on a large screen. Most firms today are using very large LED HD televisions/monitors and projecting wirelessly via their laptops.

Collaborative Technology

If you want to share an electronic file with someone outside of your office, then there must be a means for doing that without printing and shipping everything. DMS systems provide some of this functionality. It is baked into some systems like NetDocuments because they are cloud-based. If not baked in technology, then consider solutions like Citrix ShareFile.

Document Your Scanning Protocols

Every firm needs a written "here's how we do it" manual. Process documentation allows new users to pick up the system quickly. Maybe more importantly, written policies make it much easier for the firm to gently remind users who have fallen off the wagon of what they previously agreed to do. We recommend Snagit (www.techsmith.com) to document those processes by using screen shots and recordings, as well as process mapping your steps for ALL your important processes. We recommend Lucid Chart (www.lucidchart.com) or Microsoft Visio for mapping. This will become one handout for your training.

Provide Training For All Lawyers And Staff

This doesn't take long and isn't expensive, but it's critical to the success of any paper reduction initiative. Everyone needs to know how to play along. They also need to understand the "why". Without the right training, people do the craziest things (i.e., like print documents, sign it, scan and re-save as a PDF, and then send). Unless people know how to perform their core "paper" functions within a digital world, they will never give up the paper.

2 PORTABLE DOCUMENT FORMAT (PDF)

WHY PDFS ARE SO IMPORTANT

- **Worldwide Standard**: Every electronic court filing site in the country now requires the filing of PDFs. This is our new reality. PDFs have become the worldwide standard for the distribution of electronic documents. Since they are so common, it's extremely uncommon for the recipient of a PDF to be unable to open it.

- **Protect the Document**: Adobe Acrobat, and similar tools like Nuance PowerPDF, Foxit, PDFDocs, etc., allow you to protect a document so that the text cannot be altered. You can also control who may access it, whether it can be printed or opened, etc.

- **Collaboration**: Today, PDF tools make it easy to solicit feedback, comments and proposed changes to a PDF document. This makes PDFs ideal for negotiating the language of a documents and the like.

- **Easy Creation**: You can create PDFs from any computer program that will print (such as Microsoft Word). PDFs can also be created with a scanner.

- **Easy Combination**: PDFs can be compiled from many sources and any PDF can be combined with another.

- **Forms**: PDF Tools allow for the creation of fillable forms and makes it easy to collect the data that is entered into them.

PDF FILE TYPES

PDF Files

PDF (Portable Document Format) is a file format that captures all elements of a printed document as an electronic image that you can view, navigate, print, or forward to someone else. PDF files are created using a PDF writer or print driver. To view and use the files, you need the free Adobe Reader (or other free or inexpensive PDF viewers), which you can easily download for free (www.adobe.com). Once you've downloaded the Reader, it will launch automatically whenever you want to look at a PDF file. PDF files have also become the de-facto standard method for distributing electronic forms on the Internet.

PDF/A?

PDF/A (archival PDF) is a type of PDF that is used for the long-term storage of documents. Standard PDF files rely on external information, such as font libraries, to be read, and this can pose problems for retrieval far in the future. PDF/A files, on the other hand, have all information embedded in the file and do not rely on external information. This is useful for archiving, as anyone with a PDF/A reader can view a PDF/A file without the need for appropriate external information. The drawback to this is that because all information must be embedded in PDF/A files, they

tend to be larger than regular PDF files.[1] For a more detailed description of PDF/A, see the description provided by the Sustainability of Digital Formats Planning for Library of Congress Collections here: http://tinyurl.com/4wfwazy. PDF/A matters to law firms because many of the electronic case filing systems require PDF/A or may require it in the future.

Image Only PDFs

This type of PDF is visually an exact replica of the original document (whether the original document was electronic or paper-based), but it contains no text which could be searched by Acrobat or any other program. This also means that you cannot copy and paste text from the document. This is usually the type of PDF that you get when you scan a document using a copier, scanner or multifunction machine.

Searchable PDFs

This type of PDF is also an exact replica of the original document, but it also contains a hidden layer of text so that you can search for any word on any page. PDFs created from other computer programs electronically are searchable by default. In other words, if I create a PDF from a Word or WordPerfect document, an Excel workbook or an email, they are always searchable. As mentioned above, PDFs created by scanning can be, but are not always searchable. The software you're using to scan will determine whether you can create searchable PDFs. So that you can easily find the PDF documents you're looking for, you want to use searchable PDFs. See below "Searching" for a discussion on programs that will automatically make image-only PDFs text-searchable.

PDF PROGRAM OPTIONS FOR LAWYERS

There are a number of PDF programs on the market today. Here are my top recommendations that you should evaluate:

1. **Adobe Acrobat Pro DC**: There are two flavors here: Acrobat DC Pro "with services" which you can only rent; and Acrobat DC Pro desktop which you can buy. You can rent DC Pro with Services for $179.88/year or $24.99/month; and you can buy DC Pro Desktop for $449. Only Pro is available for the Mac.
2. **Adobe Acrobat Standard DC**: There are two flavors here: Acrobat DC Standard "with services" which you can only rent; and Acrobat DC Sandard desktop which you can buy. You can rent DC Standard with Services for $155.88/year or $22.99/month; and you can buy DC Standard Desktop for $299. Standard is not available for the Mac.
3. **Nuance Power PDF Advanced**: Matches features of Acrobat Professional for only $149.99. This has quickly become one of the best alternatives to Acrobat.
4. **Nuance Power PDF Standard**: Matches features of Acrobat Standard for only $99.99.
5. **Foxit PhantomPDF for Business:** Very similar to Acrobat Pro for $129.
6. **Foxit PhantomPDF Standard:** Strong match with Acrobat Standard for $89.
7. **pdfDocs Pro by DocsCorp:** Very strong feature match with Acrobat Professional and recently completely revamped. A 12 month subscription is the only way to buy it and it's $107 annually.
8. **Nitro Pro:** Matches the features of Acrobat Professional. They offer a Nitro Pro+ which is rental only for $7.99/month ($95.88 paid annually - no option to pay monthly) and Nitro Pro (desktop) which is $159.99.

[1] What Is PDF/A? See https://en.wikipedia.org/wiki/PDF/A

3 SCANNING

LARGE CENTRAL SCANNERS VS. DESKTOP SCANNERS

In most offices, it is a mistake to solely rely on large central printer/copier/scanners in the copy room. We call this centralized scanning. It results in a back log of scanning because it is an inefficient way to scan most documents. Large central scanners are fine for large documents because of their speed, but they are terrible for most documents (1 – 30 pages).

It takes on average 3-5 minutes to scan a 10-page document on a large scanner from start to final saving location, versus 45-60 seconds on a desktop scanner.

Today we are scanning less and less because so much is coming into our offices via email (or download) as PDFs. That said, we still receive quite a bit of paper, and until that stops, we will continue to need scanners. For most offices, we recommend desktop scanners for legal assistants, paralegals, and only those attorneys who express the desire to do some of their own scanning.

ESSENTIAL FEATURES OF A DESKTOP SCANNER

- Must have an automatic document feeder which holds 25 pages or more;
- You don't need a flatbed scanner because you have your multi-function copier/scanner, which has a flatbed for the rarer situation that you have a bound book or magazine.
- It must be fairly quiet (users should be able to conduct phone conversations without yelling over the scanner);
- We recommend a USB 3.0, USB-C or Thunderbolt connection to your computer;
- It must be able to scan black & white, gray-scale and color;
- It must be able to scan legal and letter sized documents; and
- It must be fairly fast (recommend 20 – 35 ppm).

RECOMMENDED DESKTOP SCANNERS

Lower Volume Daily Scanners

The following are excellent scanners that can easily handle the scanning volume for most users.

1. **Fujitsu ScanSnap iX1500.** The ScanSnap scanner is small, fast (30 ppm single sided, 60 ppm double-sided), comes with the full version of Nuance PowerPDF, and can create searchable PDFs natively. It also has a 50 sheet automatic document feeder and also includes ABBYY FineReader which will allow you to convert paper documents into documents you can edit in MS Word. It costs between $400 - $440 from a variety of vendors. It's world-class software scanning interface is incredibly user-friendly. Because it is so easy, fast & reliable, this scanner (and its predecessor, the ix-500) has made this scanner the most widely used desktop scanner in North America.

FIGURE 1

2. **Epson ES-400.** This is a TWAIN-compliant scanner that is also small and very fast (30 ppm single sides, 60 ppm double-sided). Because it is TWAIN-compliant, it can natively integrate with many programs, but the software for the end-user is not as easy to use as the Fujitsu ScanSnap Scan Manager software. I generally recommend the Fujitsu ScanSnap (above), but when TWAIN-compliancy is required, I recommend this scanner.

FIGURE 2

Higher Volume Scanners

If TWAIN-compliancy is a requirement, and you are looking for a scanner with a higher duty cycle (example: the need to regularly scan over 1000 pages a day), then I recommend looking at these models:

1. **Fujitsu fi-7160 Sheet-Fed Scanner**: This scanner is TWAIN-compliant and scans up to 60 ppm/120 ppm duplex black and white or grayscale. That is very fast for a desktop scanner. It has a 80-page Automatic Document Feeder (ADF) with enhanced hard and embossed card scanning (Example: credit or healthcare cards). This scanner usually retails for $850.

FIGURE 3

2. **Fujitsu fi-7300NX**: This is slated to replace the 7160 mentioned above although both are still available. The 7300NX adds WiFi connectivity so it can be placed anywhere and doesn't have to be physically connected to a PC in order to work. It also has a touch screen which makes it easier to scan. Otherwise, it has the same speed and characteristics as the 7160.

FIGURE 4

3. **Fujitsu fi-7180 Sheet-Fed Scanner**: Up to 80 ppm/160 ppm duplex black and white or grayscale. 80-page Automatic Document Feeder (ADF) with enhanced hard and embossed card scanning (Example: credit or healthcare cards). This scanner usually retails for $1,500.

FIGURE 5

4 DUAL MONITORS

DUAL MONITORS INCREASE PRODUCTIVITY & REDUCE PAPER

Dual monitors are absolutely needed for effective paper reduction. I understand that there some may resistance to this idea, but the reality is that dual monitors have not only become standard issue for law offices and legal departments across the country, but this concept is also a key ingredient for helping to reduce reliance on paper. Having 2 monitors simply allows you to spread out and see two things at once (like research and the document you're drafting based upon that research). Of course, it also eliminates a lot of the minimizing and maximizing of applications when you're working with two programs simultaneously. Overall, it's a big efficiency gain and I doubt you'll ever find someone with dual monitors who would ever consider going back to just one monitor. Monitors that rotate to portrait view has also turned out to be valuable to some to help review documents on the computer rather than hard copy. Many lawyers print documents in order to review them because they find it difficult to review documents on a computer screen. This difficulty typically arises out of the fact that when viewing a document on a monitor, one can only see a few paragraphs of each page because the monitor is landscape (wide) and the document is portrait (tall). To remedy this problem, we recommend buying monitors that rotate to portrait (see screen shot below). Monitors with this capability usually only cost a few dollars more than those without it and it is completely worth the extra money. As you can see below, a standard 22" monitor rotated to portrait not only allows a user to see an entire page of text at once, but it makes it nearly twice as big as it would appear if you printed it on 8.5 x 11" paper.

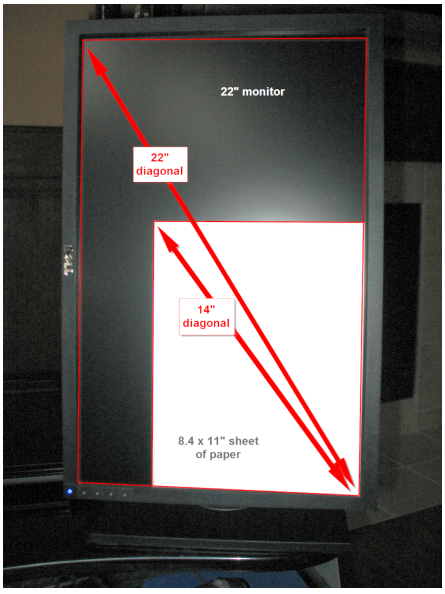


FIGURE 6

My recommendation is something like a Dell Professional 27" monitor (part number P2717H) which is $258 on amazon.com (http://www.dell.com/ed/business/p/dell-p2717h-monitor/pd). These monitors are beautiful, bright, and I guarantee will increase productivity.


FINANCIAL REPORT FY15Q2
Information
11%
3%
2%
61%
23%
SAINT HELENS
FINANCIAL REPORT FY15Q2
Information
SAINT HELENS

FIGURE 7

5 IPADS/TABLETS

IPADS/TABLETS HAVE REVOLUTIONIZED PAPER REDUCTION

One of the primary reasons that lawyers hang on to the paper file is because they don't have an effective way to bring the case/matter information with them when they go visit a client or go to court. Simply put, the iPad (and now other tablets) solve this problem 9 times out of 10.

In the 8-9 years since Apple released the iPad, it quickly established itself as a very useful tool for lawyers, and one of the biggest innovations in legal technology to come along in some time. iPads (or tablets, generally) are instrumental if a lawyer wants to take "the file" out of the office without taking or maintaining a paper file. I believe the tablet or iPad was this missing tool in our "paperless movement", and the lack of it caused us to maintain a dual filing system (maintaining our electronic file and our paper file) for nearly 20 years. Now that we have tablets, there aren't many situations where we need the paper file. We can simply carry the case file with us on our iPad. In fact, you can carry thousands of banker's boxes on your iPad. Try carrying even one banker's box in one hand!

The iPad's design is ingenious. Its functionality is equally as nice and continues to improve as legal software developers create new and innovative apps for lawyers. Indeed, the iPad remains the tablet of choice for legal app developers, far outpacing Android and Windows tablets in the number of legal apps available. Two features of iPads and Android tablets that are so appealing are (1) it is instant "on" and connected to the internet, and (2) the size, sleekness and multi-touch screen makes it many times a better experience than handling paper.

If you carry around a legal pad and a lot of paper in a legal file or Redweld, the iPad can become your legal pad and digital folder. It is truly redefining the idea of the "paperless law office", allowing you to actually carry most of your office around with you, all in a very small, light device. For courtroom work, the iPad can be used to access exhibits, pleadings, legal research, depositions, and just about any document you might need in hearings or at trial.

The iPad has some drawbacks as a computing tool that make it unsuitable as a complete replacement for your desktop or laptop; however, I believe it is ideal for courtroom use and client meetings because it is so light and easy to hold and operate. It is very easy to understand and use, with little training required. In fact, if you already use an iPhone, as so many of you already do, you'll be able to start working with an iPad right away.

Among the often-cited negatives of the iPad are (1) that it has no USB port for plugging the tablet into other devices and (2) that the battery is not removable or replaceable. One of the reasons that the lack of a USB port is not troubling is that the iPad comes with Bluetooth capability, so keyboards, printers, and other devices can be connected wirelessly to the device. Also, a number of cloud providers (NetDocuments, Dropbox, Box, OneDrive and Tresorit, among others) make it easy for you to access all of your documents online, without needing to connect your iPad to anything.

The iPad Pro has a 12.9" screen. This is one of my favorite tablets. There are some compelling features that make it worthy of consideration (at least for some users, not all). In particular, with the Apple Pencil, notetaking/handwriting on this device is an incredible experience.

In my opinion, it is this ease of use that explains why iPads are rapidly catching on with lawyers. A laptop, netbook, or even the "traditional" convertible tablet PCs, which are useful at counsel table, cannot be carried

around the courtroom easily when the lawyer is standing at the podium or addressing the jury. We firmly believe the iPad is the preferred mobile device for litigators in particular, because the apps designed for use in the courtroom are very powerful, but also simple enough that they will not distract from actually trying a case.

Essentially, the iPad is just a little heavier than a paper legal pad and not nearly as heavy as the lightest netbook or laptop.

Tablets are now integrating themselves into the workflow of lawyers, irrespective of office size or practice area, and nowhere has this been more apparent than for litigators. Whether you need to take notes, mark and handle exhibits, or manage deposition transcripts, these little computers can supercharge your trial practice. But the iPad can make any lawyer more productive, regardless of practice.

I don't think every attorney needs a tablet. In short, I think those who do more courtroom work, litigation, and those who are very mobile. One could also use a laptop/tablet hybrid (like a Lenovo Yoga, a Dell 2-in-one, etc.), but in my experience, most lawyers prefer to have a tablet separate and apart from their laptop because (1) many times you want to do tablet functions (like handwritten note-taking) at the same time you look up information on your laptop (perhaps in Legal Server, as an example; and (2) sometimes you want to just grab the tablet and leave the laptop behind.

6 SEARCHING YOUR DOCUMENTS

SEARCH PROGRAMS

One of the most common technology problems facing lawyers today is difficulty finding their documents and email. We are forced to "re-invent the wheel" because we cannot tap into the intellectual capital of our (and others') previous creations. We are constantly forced to do research over and over, and then re-write things from scratch, resulting in loss of productivity and sometimes inconsistent advice to clients.

Document management systems (DMS) solve this and many other document management problems, but a full blown DMS requires an investment of time and money. If a full robust document management solution (discussed below) is not in your budget at the moment, or just not needed right now, you would definitely benefit from a search engine or a search program in the interim. These programs crawl through entire folder structures and will create an index of every single word in every single text-searchable document going back to the beginning of time (late 80's when word processors were first utilized). It is important to note that the document must be text-based/text-searchable (see discussion below on OCR Tools).

WINDOWS SEARCH ENGINES

Copernic Desktop Search: See www.copernic.com. There are three versions of Copernic, Home (FREE), Professional ($49.95) and Corporate ($59.95). Unless you're installing it in a very large firm, you only need the Professional version. You can try the free home version, but one of the limitations of the free version is that it does not search network drives. So unless you're keeping all of your files on the C:\ of the computer you're using (I certainly hope you're not doing this), the Home version will not help you very much. Copernic will search all of your files (Word, Excel, PowerPoint, PDF, HTML, WordPerfect, text and another 150 types of files). It will also search your Outlook email and any attachments to email.

X1 Search Engine: See https://www.x1.com/products/x1-search/. Very similar to Copernic, X1 will also creating an index that is searchable in seconds. X1 retails for $96.

dtSearch: See www.dtSearch.com - $199 - one of the most sophisticated and fast search engines I've ever seen. It provides the most search options and file types that it can recognize. If you need industrial strength search capability involving enormous numbers of documents, this is your program.

Filehand: See www.filehand.com - FREE. Instantly search for files on your computer, by content. See the extracts of the files you found, even for PDF files. Scroll through the extracts so you can quickly find the information you're looking for. Find the file you are looking for, even when many files match, because Filehand Search sorts the results by relevance. Do complex Boolean searches and searches by phrase. Use it all the time because it is so simple to use!

Windows Instant Search (Windows 7 and 10): The Windows operating system has a basic, but powerful ability to search all folders.

APPLE/MAC SEARCH ENGINES

Spotlight Search (Mac OSX): This is included with the Mac OSX operating system. For more information, see http://support.apple.com/kb/HT2531

EasyFind: If you are looking for something a little more robust than the Spotlight Search, EasyFind is one alternative. Free - see http://easyfind.findmysoft.com/mac/

HoudahSpot: $15 - see https://www.houdah.com/houdahSpot/download.html.

OCR TOOLS

As discussed above, in order for a document to be searchable, it must be text based. MS-Word documents, Word Perfect documents, Excel Spreadsheets, PowerPoint files are all natively searchable because they are natively text-based. PDFs may not be IF they are generated from a scanner or copier. PDFs are searchable if they converted to PDF (using an add-in, driver, or printed from Word, Excel, or PowerPoint. If a PDF is generated from a scanner, then there is an extra step that must be taken in order for that image-only PDF to become text searchable. That step is called Optical Character Recognition (OCR). This is a process that takes a short amount of time. On average, a 1-10 page document will take 5-30 seconds to OCR. That number increases significantly as the number pages increases. Generally, this is not a function that you want to require staff to perform. It is not a good use of their time, and as a practical matter, it just doesn't get done a huge part of the time, resulting in a bunch of documents that people can't search!

Many computer users don't even know what OCR means and they just assume the search tool is broken because it is "not finding my documents, and I know it is there!" Many of these image-only PDFs come if from clients, or opposing counsel, or from a discovery production. Some come from your copier. As you may know, To address this problem, we strongly recommend a third-party back end OCR tool like SymphonyOCR or DocsCorp Content Crawler. These solutions will look at any PDF deposited in a document management system (for NetDocuments, Worldox, Epona and iManage), or a plain Windows folder structure and run the OCR function automatically. ndOCR is an add-on to NetDocuments that retails for about $3/user per month. These solutions allow you to quickly scan PDFs into the system without the time-consuming process of converting them to searchable PDFs at the time they're added. It also will OCR all your old or legacy PDFs that are currently in Windows folders and Legal Server. This may not sound like a huge issue, but it will save you and your office hundreds of hours per year. See http://symphonysuite.com. The cost of Symphony is roughly $45/user/year.

7 DOCUMENT MANAGEMENT SYSTEM

DMS DEFINED

A Document Management System (DMS) is the combination of software/hardware tools which streamlines and automates the process of document & email management. Document management software has become so useful over the past 20 years, most organizations believe it is the true foundation for knowledge management and eliminating paper in the office.

Since DMSs only manage electronic documents, any paper documents must be converted (scanned) so that they can be managed by the DMS. In simple terms, your paper "Files" are just collections of paper documents related to a particular matter. Once all of that paper is in digital form, a DMS can organize it by matter just as your paper files are currently organized.

DMS FEATURES

Legal document management software should have all the below **core functions**/features:

Easy Compliance – Integration With Major Apps

In order to be convenient to use, the DMS must integrate with Word, Acrobat (or pdfDocs, Nuance PowerPDF, Foxit, etc.), Excel and any other major application in which you save documents or files. For instance, when someone clicks the Save or Open button in Word, the DMS must intercept and ask the user to "profile" or save the document, or find the document within the DMS.

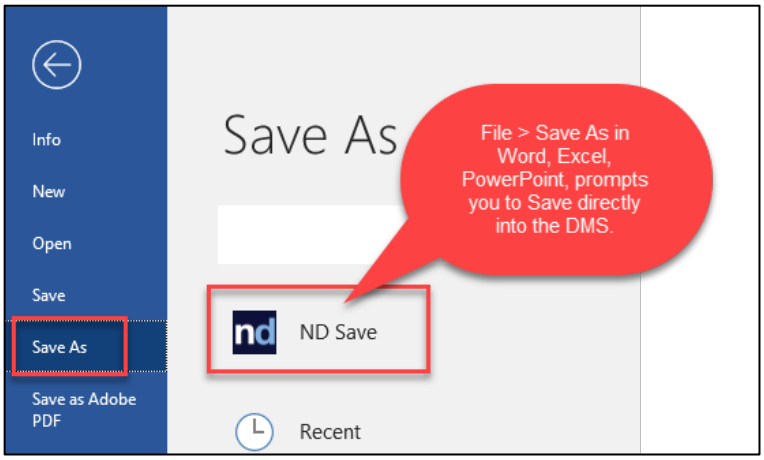


FIGURE 8

Email Management – Integration with Outlook

Email management is extremely important since most people feel crushed by email. A DMS is a full email management system (among other things). With a DMS, all emails related to a particular matter can be easily saved along with the other matter-related documents. Right now, without a DMS, users are saving emails in Outlook subfolders that no one else has access to, or they are saving emails to Windows folders through a very inefficient tedious process. Saving emails must be an easy process! Important features include:

One-click Saving: People do this constantly, every day. The process can't be time consuming, tedious or have too many steps. A good DMS solution will have integration with Outlook by selecting or opening an email and then simply clicking on a toolbar button to move a copy of the email into the DMS, as seen here in a screenshot from the Worldox document management system:

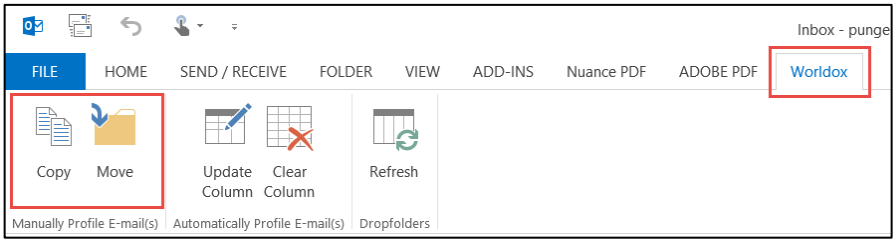


FIGURE 9

One selects an email and then hits with Copy to Worldox or Move to Worldox.

Here is a screenshot from the NetDocuments document management system:

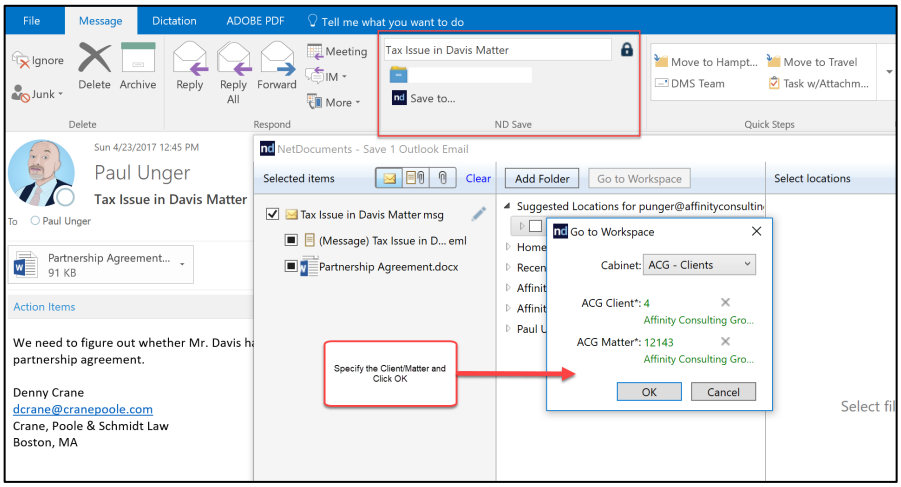


FIGURE 10

The user simply selects an email or multiple emails and using the ndSave function, can select the correct client/matter or area/matter.

Ability to save emails with attachments embedded in the native email format from within Outlook without "exporting" them or saving them somewhere else before they're moved into the DMS.

Ability to save only attachments easily into the DMS from a right-click on the email attachment and use the Save to the DMS Command as seen here with the NetDocuments integration with Outlook:

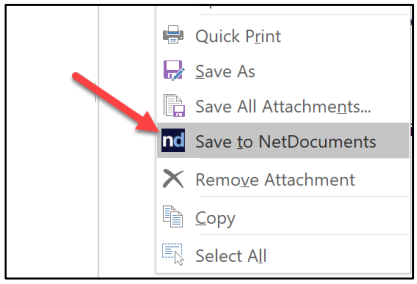


FIGURE 11

Saving Email Using Artificial Intelligence (Ai)

The NetDocuments' DMS has launched a pretty amazing new feature that uses AI to help lawyers automate the saving of email, eliminating many clicks from the above process. The feature is called ndMail. It is an optional add-on module that enhances the email filing experience from Microsoft Outlook by drastically reducing the time and effort required to save email messages into the client/matter folder.

Core to the application is the predictive email filing component which uses machine learning to determine which matter each email message in your inbox should be filed against based on the sender, recipient, subject and content from the actual message.

As a user highlights an email message in Outlook, the integrated ndMail panel will display suggested matters that it has determined may be appropriate for that email. They are listed in order based on the its "confidence" of fit. The user can then make the decision to accept, override or ignore the suggested destinations:

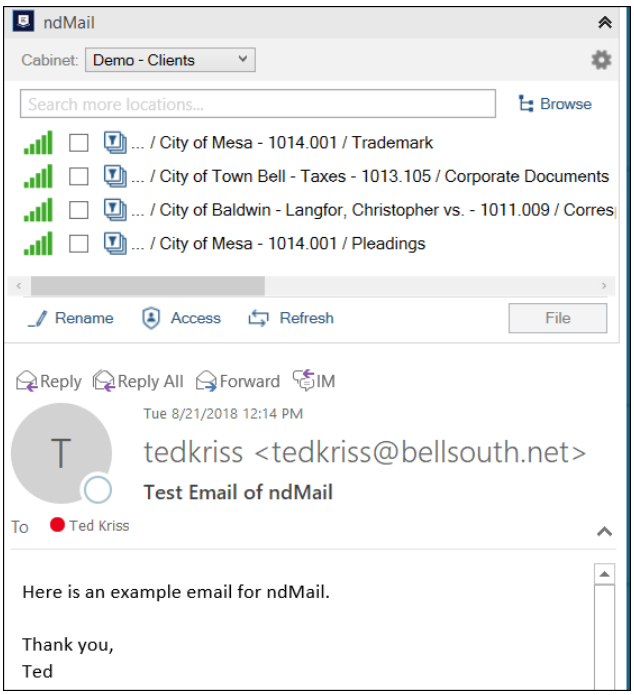


FIGURE 12

Most importantly, ndMail "learns" each time a user in your firm files an email with ndMail, which significantly increases the accuracy of suggested destinations over time across the entire firm.

ndMail also provides an email de-duplication service during the email saving process, as it reviews each message and instantly notifies the user if that email has already been saved into the system previously by anybody else at your firm.

Full Text And Boolean Logic Searching

If you have a document management program (like Worldox, NetDocuments, iManage or OpenText), you do not need to invest in a separate search engine (like Copernic, X1, dtSearch). The search engine functionality is part of the program, and within legal DMS programs, they are extremely powerful. Full text searching gives users wide-open access to their documents by framing searches based on concepts rather than categories. Users can search by many criteria - words, combinations of words, phrases, words within proximity of each other, expressions, etc. Each document matching the search terms is returned as a "hit" and the integrated file viewer will highlight each occurrence of a search term in the returned documents. This is exactly like doing

a Lexis or Westlaw-type search through your own documents. When evaluating DMSs, you want the ability to view the documents in a viewer without actually opening them, you want to be able to use Boolean logic terms (and, or, not, near, etc.), and you want the search terms highlighted in the document the system found. This is a screenshot from Worldox, who has one of the best and cleanest advanced search dialog boxes:

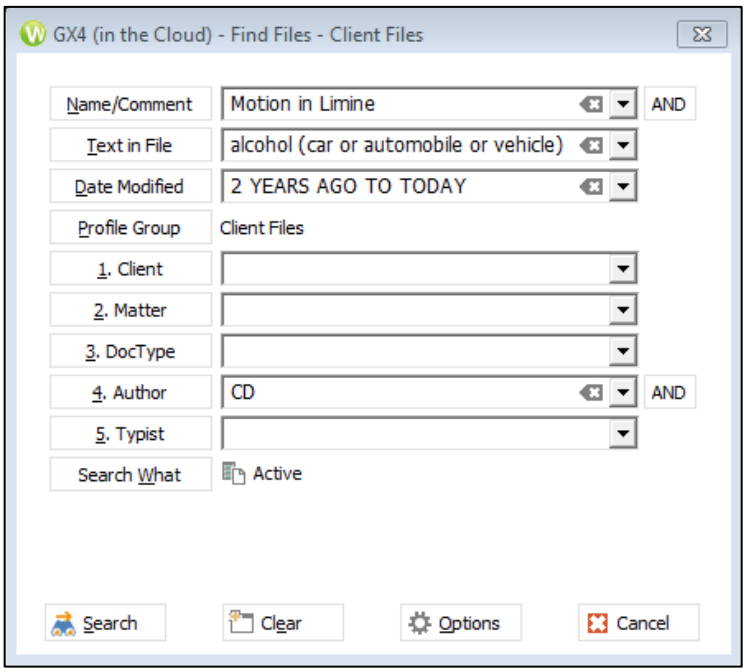


FIGURE 13

Simple Google-Type Searching

It is important for less tech-savvy people to have the ability to do quick simple searches with a "Google-Type" single search field, as best seen here in NetDocuments:

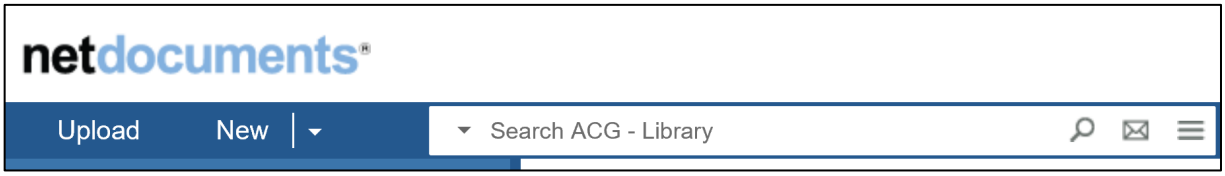


FIGURE 14

Metadata Searches

In the realm of document management, metadata is the critical additional information stored about the document (other than the file name).

Metadata includes, but is not limited to, information like:

- Name
- Comments
- User-defined "tags"
- Indexed full text
- Email From

- Email To
- Email Sent Date
- Doc ID
- Date Modified, Created, Accessed
- Cabinet
- Client
- Matter
- DocType
- Author
- Typist
- Date (actual date associated with the document)
- Date range

This search capability ensures continuity and a smooth transition when someone leaves or joins your office. For example, if someone unexpectedly (and suddenly) left your office, it would be pretty difficult to determine exactly what they were working on before they left. However, if a document management system were in use, it would be quite easy to find every single document or email that person touched in the last 90 days (for example). It's one thing to have a log or list of documents they were working on; it's quite another to actually be able to find those documents. Furthermore, the searches can be narrowed down considerably. For example, I could easily find every pleading (document type), containing the phrase "motion for summary judgment" (text in file), created by a particular employee (author), between 11/1/2008 and 11/1/2009 (date created range), for any matter having to do with the Jelson Electric, Inc. (client name). I imagine that it is presently impossible for anyone in your office to even contemplate a search like that

OCR Capabilities

As discussed above, the ability to OCR Image-Only PDFs to make them Text Searchable is critical. The DMS should be able to identify PDFs that are non-searchable and automatically OCR them to make them text searchable. This should happen on the back-end automatically, so users do not have to waste time running the OCR process on every PDF they scan or receive via email. Most DMS systems utilize add-on products like Symphony OCR or ndOCR to perform the OCR automatically.

Give Clients/External Users Secure Access to Some Documents

Systems like NetDocuments have collaboration tools natively built-in because they are designed using pure cloud architecture. In other words, you don’t need to buy an add-on product like Citrix ShareFile in order to create a place to share documents with clients. This is a screenshot taken from NetDocuments, showing this feature, which they call Collaboration or Share Spaces:

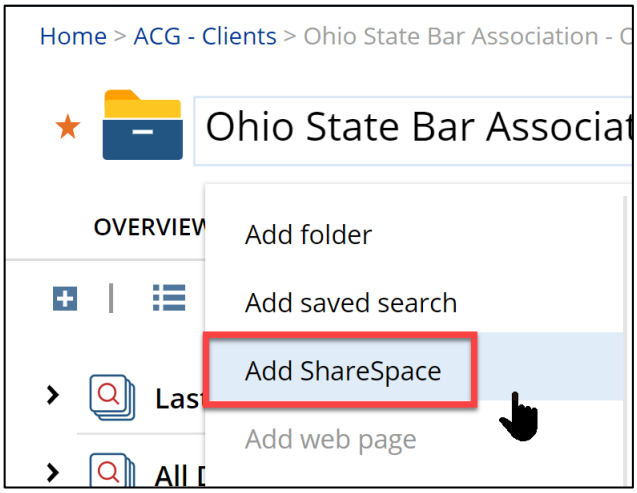


FIGURE 15

No Accidental Drag & Drops

A frequent issue reported to us is the cry for help when a document folder goes missing. Those folders are often accidentally dropped into a different folder and the user has no idea what happened. This is impossible with a document management system. Moreover, if documents do get moved accidentally, the audit trail would accurately identify what happened, when it happened, and who did it.

Deleting Doesn't Have To Mean Deleted

The office can set up a rule where deleted documents go to a 'trash' holding place where they can be auto deleted after a certain number of days or kept until an administrator empties the trash.

Organize a Library or Brief Bank

A document management system can be incredibly helpful when it comes to categorizing and protecting forms, templates, precedents and organizing a brief bank by topic that is fully text searchable. Create a dedicated cabinet that is fully searchable to tap into your organization's knowledge base.

Ability to Save Most Any File Type

The DMS must be able to hold any type of file you've created in-house as well as any type of scanned document (PDF, TIF or JPG) which will typically represent the documents you're received from the outside. A search must turn up all relevant documents regardless of physical location, format, and source application. For example, we have seen plenty of copier-based applications which only hold documents you scan. It does little good to have scanned documents in one system and all of the documents you've created in-house in another system. The idea is to get everything related to a matter in the same system, including documents you've created in-house, documents you've scanned, faxes, hand-written notes, email and attachments to email.

Version Tracking/Management

The DMS must be able to keep multiple versions of every document. This becomes very important when a document is undergoing revision and is being passed back and forth between attorneys. Most DMSs will keep over 100 versions of every document along with a detailed audit trail noting who did what to the file and when. When the revised document is saved within the system, it will prompt the user with the option to save it as another version, as see here with Worldox:

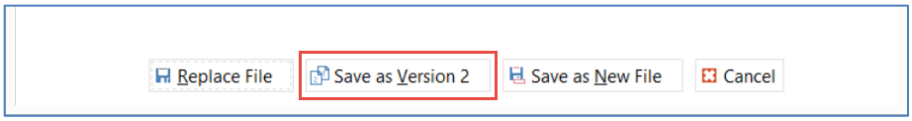


FIGURE 16

Once saved, whenever that document appears in a search result or list, the DMS groups all of the versions as one listing, and indicates that there are multiple versions available of that document, as seen here in a screenshot from NetDocuments:

FIGURE 17

If users want to see all versions of the document, they can right-click and select list versions and see a complete history:

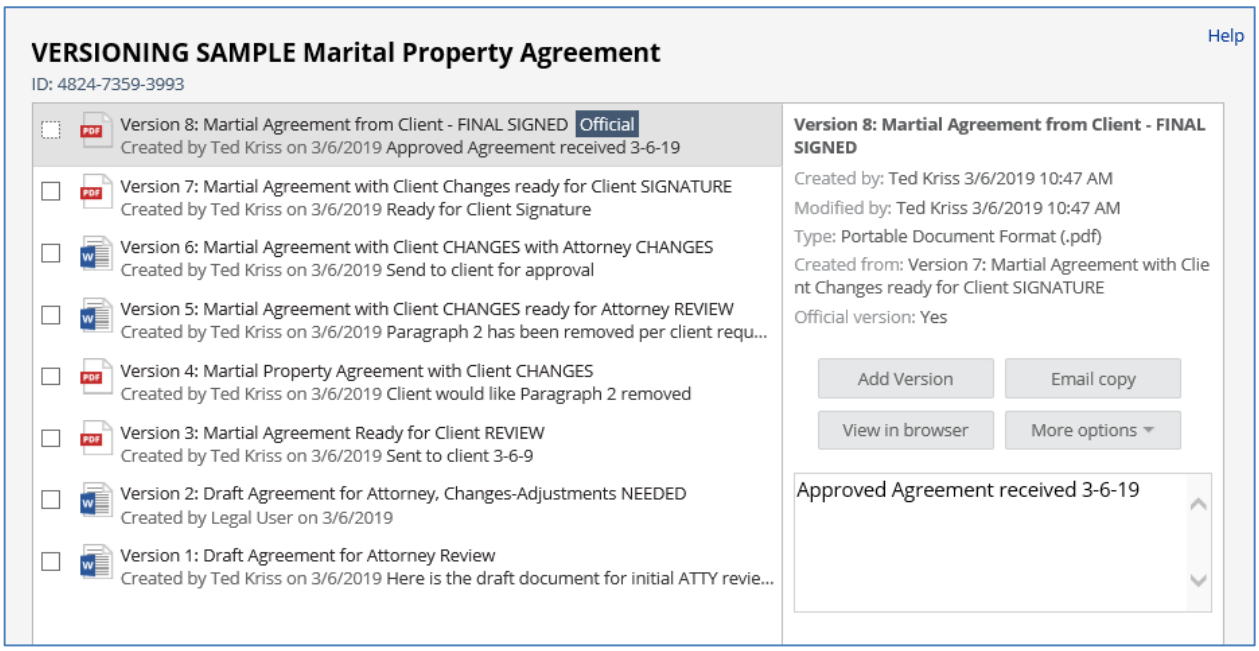


FIGURE 18

Ability to Compare Documents

Related to version tracking, users must also have the ability to compare different versions of a document or compare one document to another. In order to compare documents, some people use the compare features built into MS Word while others use 3rd party applications like CompareDocs or Workshare Professional (fka DeltaView). Since all of the documents being compared to one another will be stored in the DMS, the DMS must integrate with these functions in Word or 3rd party programs. Not all DMSs incorporate this functionality which is why this is an important question to ask up front.

Audit Trail / Document History

The DMS must be able to automatically audit all transactions related to a file saved within the system so it is easy to determine with files were first created, see everyone who touched it, and determine things like when files were copied, printed, emailed or deleted from the system.

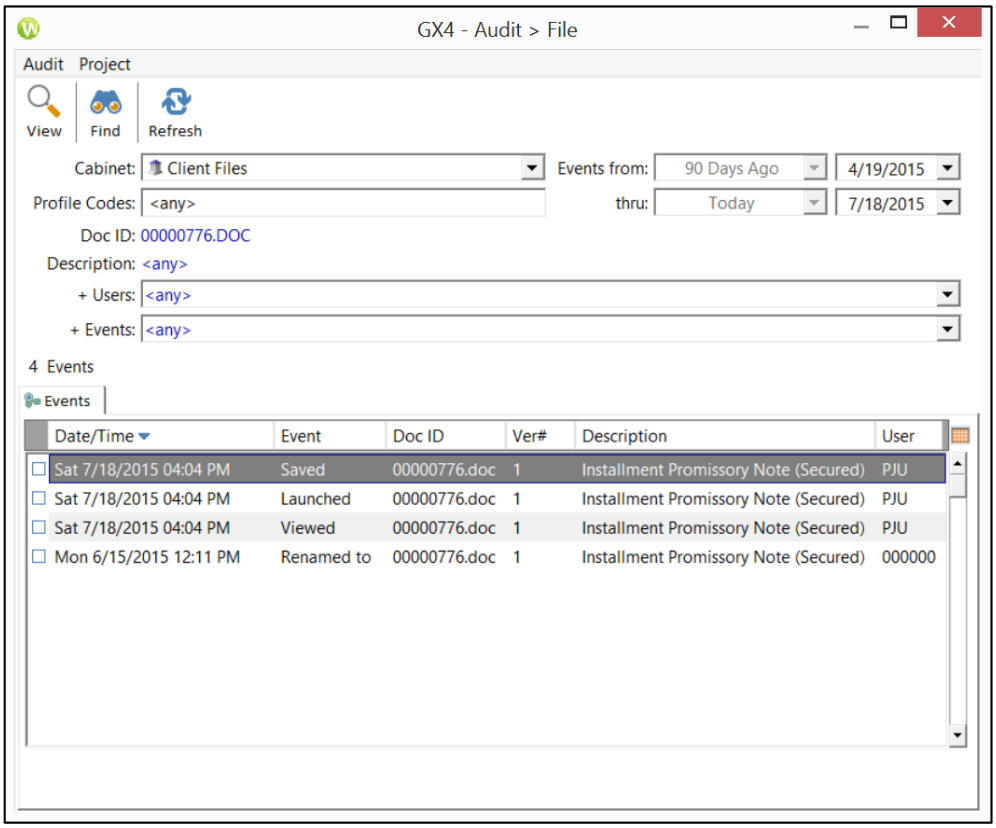


FIGURE 19

Following a Document

If you want, you should be able to have the DMS system notify you if a document has been reviewed or edited.

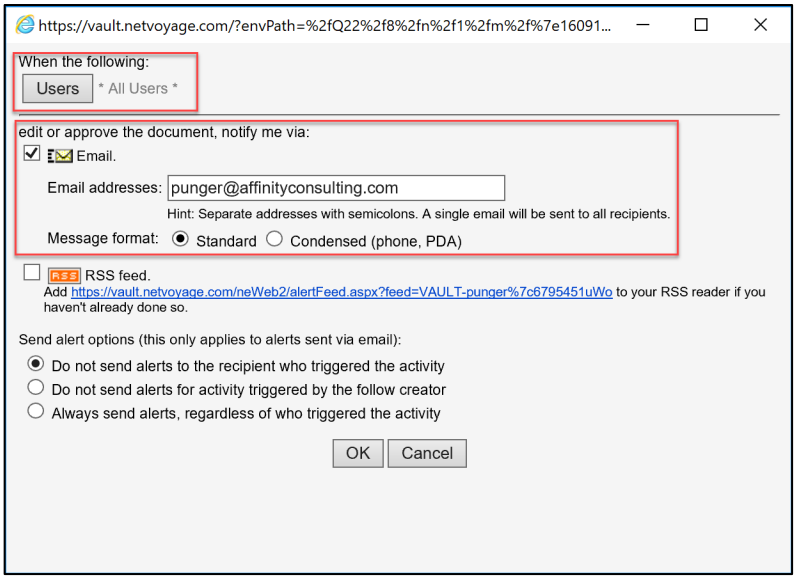


FIGURE 20

Archiving

Archiving is a means to move dated or unused files off the main storage medium to secondary storage. The DMS ensures that users can still search for information in the archived files and that there is a ready means to restore it. Many DMSs will allow site administrators to set "triggers" in the document profiles that enable automated archiving. For example, it may be desirable to set internal memos to be archived automatically after say, 24 months.

Offline Access

The DMS must be accessible when you're not in the office or if you lose connectivity … at least the most recent documents that you have touches. You will need to have full access to those recent documents. This functionality is called “mirroring” or “caching”.

Remote Access

It is critical that lawyers have access to the system via the web, from an iPhone, iPad or other mobile device. All major legal document management programs (Worldox, NetDocuments, iManage and OpenText) offer these solutions and this incredibly convenient access.

Scanning Integration

Scanned documents must be easily added to the DMS so that they are included in the document store and can be associated with matters, clients, and the like. All the major legal DMS programs have direct integration with the Fujitsu ix1500 desktop scanner. This is important because the ix1500 is the most popular desktop scanner in North America.

Consistency

The system must ensure that documents are consistently labeled and stored. This means that profile fields are drop-down lists and people don't have to manually type document types, client and matter identification numbers, etc.

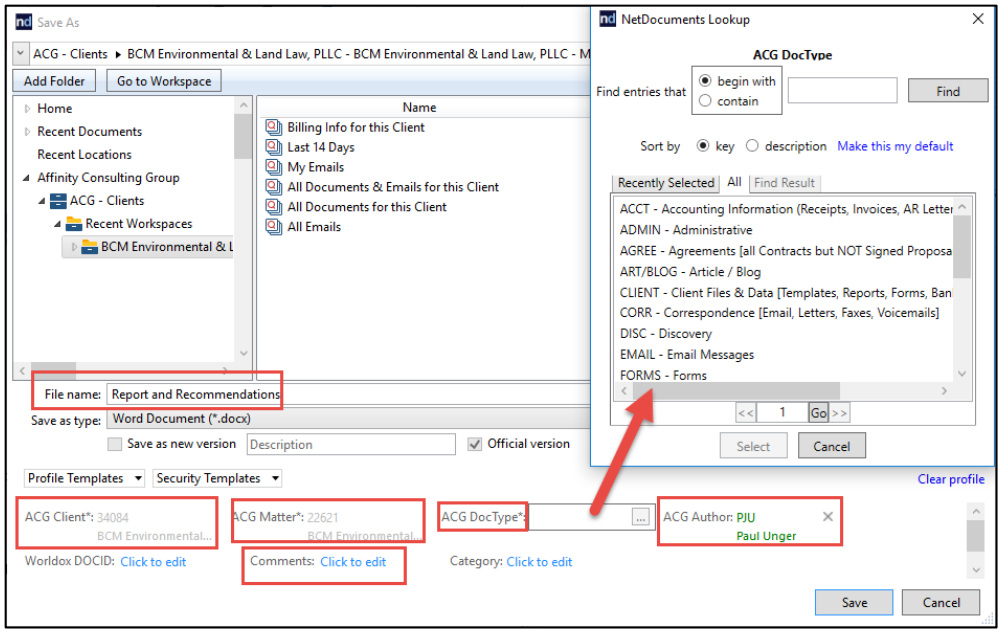


FIGURE 21

Legal DMS Main Players

I've listed below the main players in the legal market, but there are many other options:

NetDocuments: See www.netdocuments.com. This is a pure cloud-based /SaaS option and is therefore going to be less expensive up front than the on-premises options. NetDocuments is easily the most mature cloud DMS platform on the market today. NetDocuments is currently one of the most popular DMS for most firms and is a great choice for firms of all sizes.

Worldox: See www.worldox.com. Worldox is also one of the most popular DMS options. It can also accommodate larger environments, but NetDocuments, iManage and OpenText are probably better suited for very large environments (over 350 users). Worldox's core product is terrestrial (on-premises), but they do offer a hosted hybrid cloud solution.

Epona: See https://www.epona.com/dmsforlegal/. Epona is a fairly new pure-cloud/SaaS DMS program that uses Microsoft SharePoint as it's behind the screnes repository. It is well-suited for firms of all sizes.

iManage: See http://www.imanage.com. iManage is an excellent program, but it tends to cater to large enterprises. iManage's core product is terrestrial (on-premises), but they do offer a hosted hybrid cloud solution.

OpenText (formerly Hummingbird): See http://www.opentext.com. Like iManage, OpenText tends to cater to large enterprises also. OpenText's core product is terrestrial (on-premises), but they do offer a hosted hybrid cloud solution.

8 DOCUMENT MANAGEMENT WITHOUT DM SOFTWARE (HOME-GROWN DMS)

From a productivity standpoint, an enormous amount of time is collectively wasted daily in law firms and legal departments searching for documents when documents are managed poorly. Unfortunately, in our experience, most organizations, no matter the size, have poor document management practices if they do not have document management software. It's simply too hard to police and monitor to make sure that people comply … ie. Saving documents in the central designated location and doing so in a consistent manner. As the firm size grows, so does the need and justification for a DMS. That said, sometimes there isn't money in the budget right now. So what can you do in the interim? What are the essential elements?

CENTRAL FOLDERING THAT IS MATTER-CENTRIC

It is critical that documents are saved by **client/matter, or within a legal department by area/matter**, and not by user. Saving documents by user can create lots of problems, such as:

- Documents for one client being located in more than one folder.
- Revision conflicts.
- Losing things permanently if staff turns over. Turnover creates an administrative nightmare for everyone in managing those documents. Saving by user results in duplicate files and no one really knowing what is the authoritative version of a document or how matters were left.

Saving documents on a user's local hard drives is a big no-no as well. Those documents are not getting backed up! They need to be saved centrally on a file server or in the cloud, within one matter folder. You can create a logical directory layout, find documents easier, and it makes backing up your documents simpler. You can use Windows active directory security to limit access to folders based on users.

If S is your server drive where your documents are located, you may create something like:

- S:\Clients
- S:\Accounting
- S:\Marketing
- S:\Admin
- S:\Library

It would look something like this:

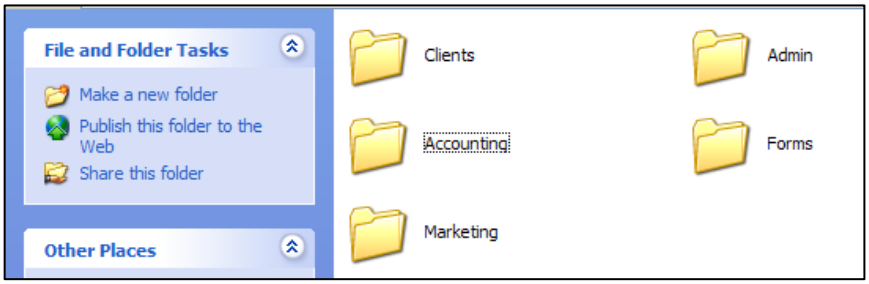


FIGURE 22

If S:\ is your server drive, you'd create a folder called S:\Clients, and sub-folders for each client thereunder:

- S:\Clients\Carsey, Joe
- S:\Clients\Cochran, Doug

Within the specific client folder, you would have a subfolder for each matter.

S:\Clients\Smith, John\Real Estate - Sale of 123 Maple St

- S:\Clients\Smith, John\Real Estate - Purchase of 400 E Main St
- S:\Clients\Smith, John\Divorce

Within each matter, you would have a subfolder for each document type (correspondence, memos, pleadings, etc.)

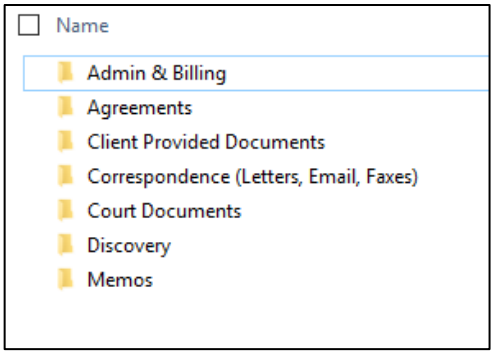


FIGURE 23

We recommend keeping an empty set of these folders and then pasting them into each matter/case created so that you have a consistent folder structure for all of your matters/cases. This will also make it much easier later down the road if you decide to purchase a full-blown legal document management system. Migrating documents to the new system will be much easier.

SOLID NAMING SCHEME

Just like the paper file, most people would like everything sorted by true chronological date. To accomplish this, precede every file name with a date, year first. If you enter the date month/day/year, then all of the January files (for all years) are lumped together, all of the February files are together, etc. Recommended naming convention:

2020-10-30 - Letter to Rob Miller re Jared.docx

2020-09-10 – Letter to Jared re Paula.docx

2019-01-14 – Letter to Judge Smith re Nothing in Particular.pdf

The date indicates the date the document was mailed out if it's a letter; and the longer description makes it clear what this document contains without even opening it.

SEARCH ENGINE

If a full robust document management solution is not in your budget at the moment, or just not needed right now, you would definitely benefit from a search engine or a search program in the interim to find documents saved in the above-referenced folder structure. These programs crawl through entire folder structures and will create an index of every single word in every single text-searchable document going back to the beginning of time (late 80's when word processors were first utilized). See above *Searching Your Documents – Search Programs*.

Cybersecurity Policy

HANDBOOK

ACCELLIS
TECHNOLOGY GROUP

TABLE OF CONTENTS

Introduction

A law firm with four partners and a staff of ten is breached as part of an indiscriminate attack from a bot-net – a large group of computers infected with malicious software and controlled without the owners' knowledge – by 20-something year olds in Eastern Ukraine.

The vector of attack exploited outdated Adobe software on an attorney's laptop. The malicious code executed behind the firm's firewall and before encrypting all of their data to be ransomed back, the code scoured the network for personally identifiable data, such as social security numbers, dates of birth, and home addresses and copied it back to the hackers.

Within weeks, employees of the firm were well in the midst of dealing with identity theft to the tune of millions of dollars. And within three months, several of the staff filed suit against the partners for not doing enough to mitigate a cyber-attack or the resulting damages.

This is a scenario that is beginning to play out with greater frequency. For too long, firms have turned a blind eye to the growing threats to the cyber security of firm and client data. The attacks have grown more sophisticated than what a firewall and some anti-virus software on a desktop can handle.

The American Bar Association (ABA) has taken notice. To address the security needs of the legal industry, ABA Resolution 109 specifically recommends:

> ***That … all private and public sector organizations develop, implement, and maintain an appropriate security program, including:***
>
> *(1) conducting regular assessments of the threats, vulnerabilities, and risks to their data, applications, networks, and operating platforms, including those associated with operational control systems; and*
> *(2) implementing appropriate security controls to address the identified threats, vulnerabilities, and risks, consistent with the types of data and systems to be protected and the nature and scope of the organization*

Written security policies are the first step in demonstrating that your firm has taken reasonable steps to protect and mitigate the ever-growing threats to the firm's cyber security. This guide is intended to provide law firms with a list of the most urgent policies they need, why they are needed, and how to use them.

Based on the ISO 27001 standards for securing assets such as financial information, intellectual property, employee details or information entrusted to firms by third-parties, this handbook will outline where policies fall in the grand security scheme (which layer) and will outline the five categories of policies law firms need: overall security program and awareness, data handling, access to systems and sites, monitoring, and securing.

A Layered Approach to Cybersecurity

Layered security, or what is also known as 'Defense in Depth,' refers to the practice of combining multiple security controls to slow and eventually thwart a security attack. It's an approach recommended for law firms of nearly any size.

By combining a myriad of hardware, software, policy and assessment tools, a firm can significantly decrease its risk exposure. More simply, each attack vector at the firm is assailable, but those that are not part of a layered approach are most at risk. Let's begin by understanding the layers at hand.

1) Data - This is the sensitive information you house like SSNs, DOBS, financial records, merger & acquisition files, patents, trade secrets, contact lists and more.

   Relevant questions: Where is my data in space and time? On what specific drives? Utilizing what database technologies? Accessible remotely by what tools and people?

2) Application Security - These are the controls within your line-of-business applications like practice management, time and billing, accounting, document management, e-discovery, and so on.

   Relevant questions: Have we setup security profiles, access rights, permissions, ethical walls and passwords? Do we have or need dual-factor authentication? How are we sharing important documents and emails with clients?

3) IT Infrastructure Security - These are the actual hardware and software assets you employ for security like antivirus, antispam, firewall, content filtering, patch & vulnerability management, encryption, physical security and more.

   Relevant questions: Am I proactively managing security? Is the firewall fully employed or is it just on? Are we testing for new vulnerabilities on an ongoing basis? Do we have encryption for data at rest?

4) Education & Policy Enforcement - Refers to what we are here for today; the creation of firm policies and plans that constitute the firm's Cybersecurity Framework, such as written security policies, incident response plan, disaster recovery plan and more.

   Relevant questions: Are firm members trained on proper security? Do they know how to identify a malicious email or how to respond if they believe a virus has infected their PC? Are our policies adequate, written, updated and enforced?

5) Continual Assessment & Improvement - Finally, firms need an ongoing process for the testing of new attack vectors, the effectiveness of the CS Framework, and testing for weaknesses in the approach.

Relevant questions: Have new threats emerged? Do recent close-calls warrant a review of our practices? In spite of our efforts and security spend, are users really knowledgeable and therefore safe? Have any of the new programs or services we purchased this year compromised our security posture?

The purpose of this handbook is to assist firms with one of the imperatives within the Education & Policy Enforcement layer: the creation and use of policies. As mentioned, there are five categories of policies, which we will review now: overall security program and awareness, data handling, access to systems and sites, monitoring, and securing.

Overall Security Program & Awareness

The basis of any effective security program starts by defining the goals of the program, defining roles and responsibilities, establishing an incident response plan, and developing and conducting continual education to re-inforce the policies and controls.

A. Written Information Security Policy

A Written Information Security Policy (WISP) defines the overall security posture for the firm. It can be broad, if it refers to other security policy documents; or it can be incredibly detailed. Some firms find it easier to roll up all individual policies into one WISP. For example, you might find it easier to list out all of the policies for securing your firm's IT resources, such as passwords, mobile device management, email, etc. and simply write a paragraph of guidelines that firm member must follow.

The key components of a WISP include:

- Asset Inventory - This is an organizational evaluation of all informational assets the firm maintains including sensitive client and employee data
- Threat Assessment - This is an evaluation of what threats exists to those assets
- Disaster Recovery Plan – This is a technical plan that is developed for specific groups to allow them to recover a particular business application; ie, network share drives, practice management solutions, etc.
- Breach Notification Plan – This is a guideline for all critical parties if the firm's network is breached. It should include notification plans and contact information for authorities and client contacts and possibly credit monitoring services
- Security Awareness Plan – This is a training and management plan the outlines procedures for identifying unknown resources in the building, email security, required encryption, smart phone guidelines and safe Internet browsing.
- Guidelines for updating and testing the WISP on a regular basis

Real world use: Your city has an extended power outage, or your building burns down, or you suffer a data theft - what do you do? Who do you notify? Having a WISP means having a plan.

B. Roles & Responsibilities

In the event of a security incident, you simply will not have time to figure out who is responsible for what. If there is any hope in mitigating the damages related to a breach, swift action is paramount. The roles & responsibilities policy has one sole purpose – to outline who will approve the information security policy, assign security roles, coordinate and review the implementation of security across the organization.

The policy should define the make-up of the Security Team/Committee and should include a decision maker and a representative from the IT group. Responsibilities, such as those for internal control accountability, overview of systems management and prevention, and incident response should be assigned and written out.

Real world use: Cryptolocker encrypts all firm data, who notifies users to log out? Who contacts the IT department? Who contacts affected clients?

C. Incident Response and Security Event Plan

Having (and practicing) an incident response plan is probably one of the most crucial steps any organization can take. It is not a matter of *if* an incident will occur, it is *when* an incident will occur. Having a plan in place will significantly reduce the impact to the firm. A good and well-rehearsed plan will reduce the risk and exposure to the firm, clients, employees, and partners that may arise out of a data theft or data loss incident. Law firms have a duty to protect entrusted information and to properly respond to an incident.

The purpose of the security event plan is to define when an incident response plan is to be enacted. This policy is designed to reduce the exposure that may arise out of a data theft or data loss incident. The policy details the nature and scope of an incident and identifies what client information systems and types of personally identifiable information have been accessed or misused.

According to the American Bar Association, if you find that your confidential information has been breached or exposed, you are obligated to (Bro & Smedinghoff, 2014):

1. Investigate and remedy the problem
2. Notify persons whose personal information was compromised
3. Notify state enforcement agencies
4. Notify Credit Agencies

Most states expect these steps to be handled as quickly as possible. It is important to know that encrypted data represents a safe harbor from these rules. Also, specific rules can vary from state to state so be sure to research your responsibilities when creating your WISP.

A good plan will describe the necessary steps to be taken in the event of a computer emergency, network intrusion, and/or data loss – including identifying a security response team, procedures for responding to an event, identifying the point of the breach, mitigating damages, communication to firm members and clients, and when to involve law enforcement. One of the most important, but often skipped, parts of an incident response and security event plan are the schedules and procedures for testing the plan.

Real world use: Your servers experience drive failure and are out of warranty. You start the process of spinning an image in the Barracuda cloud and are back online. You operate several days this way before realizing you still haven't ordered the replacement hardware. Now you are several days behind the eight ball.

D. Security Awareness Training Policy

Education and enforcement is critical to the success of the firm's security program. All firm members should be well versed and fully comprehend the tools and policies in place to help protect sensitive firm data. The policy should enumerate all the necessary steps the firm will take to empower firm members, such as regularly scheduled security classes and white-hat testing to verify all the roles and responsibilities are fully understood.

Consider offering a mandatory security class, at least on a semi-annual basis. Establish a communications channel to provide updates to the information security policies and recent threats to firm members. As part of the security awareness training, conduct "pop quizzes" throughout the year to make sure users are following the proscribed policies.

Real world use: A firm wants new employees trained on proper security; what kind of security training will there be for practice management, time and billing, remote access, etc.? How does the firm intend to raise awareness of phishing and socially engineered attacks?

Data Handling

Data is at the heart of the matter when it comes to cybersecurity. Personal identifiable information (PII), client data – most of which is protected by attorney-client confidentiality, and financial information all represent what amounts to data gold. Policies and procedures that govern how data is handled – knowing how to classify data, how it is accesses, and the full life cycle of a record is essential.

A. Backup & Recovery Policy

The firm's data is only as good as its last test restore. The backup and recovery policy should describe in detail all the requirements and procedures for maintaining and recovering backup copies of private and confidential data. The policies should detail the schedules, media, and recovery procedures – including testing restoration of data on a regular basis.

The policy should detail what data is backed up, how it is backed up, where it is backed up to, and when it gets backed up. Two rules of thumb for backups: 1) Use a backup rotation such grandfather-father-son (GFS) or Tower of Hanoi in order to distribute the backups across a wide set of media, 2) Follow the 3-2-1 backup methodology which states there should be at least 3 copies of the data, on at least 2 different types of media, and at least 1 copy is stored offsite. The policy should also describe the test recovery procedure and schedule.

Real world use: A firm loses all their data; they go to their backups to find none are recoverable; now we're in real trouble. A proper backup plan includes periodic fire drills – that is, attempts to restore backup media to make sure backups are working.

B. Data Classification & Handling Policy

In efforts to minimize the unauthorized sharing of classified information, data handling and classification of that data set is required. Firm management would approve this information security policy, assign security roles and coordinate and review the implementation of security across the organization.

The protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal and State law.

The policy should provide guidance of how data is classified and what level of dissemination is allowed. Typically, the policy contains a grid similar to the following:

Record Type	Restricted	Public
Client matter	X	
Blog article		X

Real world use: A firm has a policy of sending important information by encrypted email only; but what is considered 'important'?

C. Data Disposal & Data Retention Policy

This policy describes retention and destruction of physical and digital documents based on record-keeping requirements and practical business needs. This includes limiting data storage amount and retention time based on what is required for legal, regulatory, and business requirements; process for secure deletion of data when no longer needed; specific retention requirements for PII data; identifying and securely deleting stored sensitive data that exceeds defined retention requirements.

Take stock of the types of different records, where they are stored, and how much you have. For example, personnel records might be stored on paper in the file cabinet of the HR manager while financial and client data are all in electronic format. Each record type and how it is stored will have ramifications on how the record's life cycle will be managed. Different records in different forms require different periods of retention. There can be many types of records (HR, business, client, financial, etc.) and there are two forms (electronic and physical). Know the laws and regulations for certain types of records. The policy should define the rules that move records from online (production) to nearline (easily recoverable) to offline (offsite and archived).

Real world use: A firm replaces servers; the old servers are too old to keep; what should they do with the hardware? Where does it go? Should the drives be electromagnetically wiped?

Access to Systems

Firm members access data to create solutions for clients - this is the essence of practicing law. Policies that establish methodologies for accessing data and other critical systems need to be secure while allowing ample affordance to firm members.

A. Accounts Management Policy

Establishing the procedures for maintaining accounts and credentials to all systems is as basic as it gets. Accounts and user IDs must not be left available to users who no longer need access to firm systems. This policy defines the control requirements for the secure management of accounts on firm assets and communication systems.

When creating the policy, be sure to include standards for unique identification, such as a username. Define rules for account that have full control of information, such as system administrator accounts. Establish guidelines for account creation and removal.

Real world use: A firm wants to improve its security but has no policy for passwords. In absence of a policy, how will users manage password expiry, strength, rotation and multifactor authentication?

B. Acceptable Use Policy

Most firms have some sort of acceptable use policy already in place. This policy defines the activities that are permissible when using any firm assets, including but not limited to, computers, workstations, laptops, mobile devices, tablets, or any device that can communicate with firm systems. This applies to all users of firm information assets including but not limited to firm employees, partners, third-parties, interns, or guests of the firm. These rules of behavior apply to the use of firm-provided IT resources, regardless of the geographic location.

When writing an acceptable use policy, include guidelines that discuss how firm members should use company equipment, service such as email and Internet access, how they utilize social media, and appropriate responses.

Real world use: A firm wants to minimize socially engineered attacks but users are angry at losing social media access; is Reddit okay? What about Engadget? CNN?

C. Software Usage Policy

In most cases, firms do not own the software they are using. Typically, it is licensed from a variety of vendors and other sources, such as Microsoft. In order to guard against proliferation of data and software, the Software Usage policy defines the requirements for compliance with software license agreements and related copyrights on all firm computer and communications systems.

Along with detailing software licensing and usage restrictions, the policy should cover other areas of software management such as installations guidelines, procurement procedures, and support agreements.

Real world use: The software a firm has is expensive and powerful; it can do a lot; too much sometimes. What controls do you have in place to prevent users from circumventing security?

D. Systems Access Policy

The Systems Access Policy defines the requirements surrounding access to the all firm data and systems. The policy governs aspects of recording who accesses data and systems, when the access takes place, permissions to application and data, and other privileges granted by the firm.

Include policy statements that cover control to overall access to firm's systems. For example, specify access restrictions, user accountability, guidelines for controlling access, and system privileges. Be sure to include this policy as part of the overall security awareness training.

Real world use: There is no policy distinction between staff and partners in Worldox; both have access to all financial information. With a proper SAP roles are assigned to user groups to prevent staff from seeing (let alone unnecessarily searching through) information they do not have rights to.

E. Physical Security Policy

The Physical Security Policy should describe how the physical location is accessed, including all points on ingress and egress. If there is a video surveillance system, include the procedures for rotating times or video storage. Other times to consider when drafting the policy are equipment maintenance, cable security, environmental controls, intrusion protection, and facility structure.

Access to the physical offices or datacenters where the firm's IT infrastructure is housed should always be locked down.

Real world use: To maintain HIPAA compliance firms need a locked server room; if you work with hospitals and people have access to your server room like they do a national park, are you at risk?

F. Vendor Compliance Policy

Some of the more recent high-profile breaches did not occur by hacking through a corporate firewall. Instead, access to the internal networks were attained by a malicious actor posing as a third-party vendor to perform maintenance on site. This policy defines the requirements for establishing physical location and protection controls at firm facilities to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Your vendor policy should cover the general guidelines third-party vendors will follow as it pertains to protecting firm data. Managing the list of approved vendors, including regular re-authorizations, vendor access – both in physical and virtual contexts, and controlling access to as few firm recourses as necessary for the vendor to complete the job.

Real world use: Target was hacked by one of its repair contractors. Do your third-party party vendors and partners comply with basic Internet security practices?

Monitoring for Incidents

There is a plethora of activity on firm networks, some of which is benign, some is malicious. Firms require policies and procedures to constantly monitor activity and offer both preventive and detective controls.

A. System Management Policy

The Systems Management policy defines the requirements for managing defaults configurations and changes to firm applications, computers and communications systems. It should outline access restrictions, session controls, authorization controls, awareness training and vulnerability management.

This policy should include information statements on items such as single-function server, asset inventory, and baseline standards. Policy statements for managing the IT infrastructure should cover remote management, vulnerability scanning, patching and bug fixes and updating core systems and software.

Real world use: When does a suite like Amicus Attorney get upgraded – whenever you feel like it? When does it get patched – sooner? What is your plan for sudden data corruption? By managing these reactively you are wasting precious resources.

B. Monitoring Policy

As activity is logged, requirements for managing and monitoring the data that are generated by the firm's information technology infrastructure are defined in this policy – including planning, contents, retention and maintenance of log systems at the firm.

Monitoring policies need to identify the systems and controls that require event logging. Thresholds, once established, should be set so alerts and remediation can take place as soon as possible. Log maintenance and storage should be included as part of the backup and recovery plan and be available for the incident and security event plan.

Real world use: You provide employees with phones and an Exchange sync of client data; do you also have the authority to monitor GPS location? Perform a remote wipe? Decide and formalize this in a policy so when you need to do your job there is no ambiguity.

Securing Technology Resources

From mobile devices to social networking to the common desktop, firms use what can seem like a dizzying array of technological resources. As instrumental as those resources are to conducting business, each of them can serve as a vector of attack for hackers. Securing them through software and policy is a must.

A. Anti-Malware Policy

Malware is software written with malicious intent. Computer viruses, Trojan horses, worms, and spyware are examples of malware. The policy states the requirements for controls to prevent and detect the dissemination of any malicious software on firm computer and communications systems found on firm assets.

The anti-malware policy governs the centralized anti-malware system in place at the firm and should include guidelines for updates, rules for quarantining and/or removal, and communication efforts if malware is detected.

Real world use: Malware can be installed by clicking a link in a phishing email, or by clicking an ad that looks legitimate, or by other means. In order to effectively combat this attack vector, you will need to establish rules for using IT at the firm.

B. Clean Desk & Clear Screen Policy

Clean desks are the cornerstone of a secure workplace. In efforts to minimize the unauthorized sharing of classified information, clean desks are required. Guidelines are needed to accomplish clean desks and clear screens. Statements regarding screen locking and the use of post-it notes that contain sensitive information are a part of this policy.

C. Cloud Services

This policy applies to all external cloud services (e.g. cloud-based email, document storage, etc.). Personal accounts are excluded. This policy provides guidance for how to handle any services related to remote servers storing sensitive firm data.

The cloud services policy should layout the firm's position of non-managed cloud services, such as Gmail or DropBox. Expectations that work-related materials should not be transmitted over non-managed cloud services is a critical part of the policy.

Real world use: Many firms have consumer tools like Dropbox, Box, Drive and other cloud apps. Staff and partners alike may be unknowingly exposing your sensitive data. Having a policy forces everyone to uses industry best practices.

D. Email Policy

Email is the primary means of communication at the firm. Guidance is necessary for compliance reasons as well as congruity. This covers passwords for emails, acceptable use for emails, content restrictions, backup and monitoring.

Consider including policy statements as it relates to email that discuss acceptable content to be shared over email, email encryption, phishing and attachment handling.

Real world use: A firm wants to find all emails related to a case; they can perform a conflict check and export records, but wouldn't it be helpful if employees already had this information readily available? An email policy for retention can standardize the ways you save making finding what you need that much easier.

E. Encryption Policy

This policy defines the requirements for establishing the encryption implementation and management requirements related to the firm computer and communications systems infrastructure. By setting standards, the firm maintains the most relevant encryption technology is used.

Define places within the firm infrastructure where encryption is warranted, such as laptops, email, HR data, and other places where critical or otherwise sensitive data is stored.

Real world use: A firm has emphasized data encryption as an asset in its war against cyber criminals. But Sheila has no password on her phone where some of that data resides. Hackers log into her phone and bypass encryption. A policy ensures you can adequately defend against this attack vector.

F. Mobile Device Policy

Mobile devices are assets that the firm utilizes on an everyday basis. This policy determines the information security requirements for the protection of sensitive information while being transmitted or received over any type of mobile device.

A mobile device policy should detail how mobile devices are issued and managed. Password and access controls should also be defined. Mobile app installations guidelines and mobile device wiping and reset guidelines should also be included.

Any features of Mobile Device Management (MDM) plan should be documented: encryption, password expiry, content filtering, whitelisting, and more. Moreover, each class of data available to the device should be defined and policies around it enforced (i.e., Exchange sync, mobile app, emails, etc.).

Real world use: A firm has mobile devices with client, event, and task data. A phone is stolen and the attorney knows an important merger and acquisition document was present on the device. How can the data be removed?

G. Password Management Policy

Passwords are the primary token used to access firm information systems. How passwords should be handled must be properly coordinated and supported. Outlining specifics on how passwords should be managed by each employee is central to staying secure and compliant.

Password policies should describe how user passwords are created and managed. Include definitions on acceptable password characteristics such as password length, complexity, and a password-change schedule.

Real world use: A firm has one password to log on to Windows which enables password-free login to all applications and databases. The password hasn't been changed in three years. Worried yet? Maybe the password is 'password' – how about now?

H. Removable Media Policy

This policy defines the requirements for the proper handling of all media that contains firm information. In most organizations, information is generated and stored on many different types of media including paper documents, computer media, and a myriad of portable devices. Much of this information is considered confidential or sensitive, which requires that its handling is performed in a safe and secure manner.

The removable media policy should detail how the firm and firm member handle removable media such as USB drives and DVDs or CDs. Consider creating statements that restrict or control the use of USB thumb drives.

Real world use: A firm has prohibited using flash drives to store information of any kind, but has no media policy in place and therefore has implemented no security controls. This means the firm is relying on the honor system rather than using centralized management to disable the use of any media.

I. Social Media Policy

Social Media is a predominant part of popular culture and becoming an integral part of business. Firms use social media as means to advertise and keep in touch with clients. Firm policy statements on social media should protect the firm from the dissemination of sensitive information and/or damaging the firm's reputation.

Real world use: a firm encourages staff and attorneys to have a social media presence. A staff member happily announces to her 500 followers that the firm is helping merge two pharmaceutical companies. This sends one of the company's stock prices into a spiral and jeopardizes the deal; the company is talking about suing the firm for its market value loss.

J. Wireless Communication Policy

Firm members are constantly part of a connected world. This policy addresses the use of mobile communication devices via wireless communication either Wi-Fi internet or Bluetooth for business purposes – and methods for securing the communicated information.

This policy should describe how the firm protects its assets from unauthorized access over Wi-Fi and other wireless vectors. Statements should include the firm's position on personal hotspots and use of guest networks.

Real world use: Staff members are pressed for time so they decide to use Wi-Fi direct to transfer a document to an attorney. Problem is, the channel was poorly setup and the document is intercepted by opposing counsel just hours before trial.

Cybersecurity Policy Templates

A. Sample – Security Event Policy

See page 17

B. Sample - Social Media Policy

See page 29

C. Sample - Systems Management Policy

See page 33

Policy Title	Security Event Policy
Policy Number	ABC-123
Effective Date	INSERT DATE POLICY BECOMES ACTIVE
Responsible Office/Person	Security & Compliance Officer
Related Policies	ABC-321; ABC-456

I. Contents

II. BACKGROUND

The ABC Firm Security Event Policy has been developed to define when an incident response plan is to be enacted. This policy is designed to reduce the exposures to ABC Firm and the consumers, employees, and partners of ABC Firm that may arise out of a data theft or data loss incident. ABC Firm has an affirmative duty to protect consumer information and to properly respond to incidents. ABC Firm assesses the nature and scope of an incident, and identifies what client information systems and types of personally identifiable information have been accessed

or misused. ABC Firm will refer to ABC-321, Incident Response Plan to contain and control incidents to prevent further unauthorized access to, misuse of, consumer information, while preserving records and other evidence. Notifying appropriate law enforcement agencies will only happen if required by law.

III. SCOPE

This policy applies to the entire ABC Firm team, including the President, Director, employees, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with ABC Firm, as well as volunteers and guests who have access to ABC Firm assets. Assets include but not limited to, workstations, servers, mobile phones, software, data, images or text owned, leased, or utilized by ABC Firm.

IV. DEFINITIONS

Policy – A policy is a governing set of principles that guide ABC Firm practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances the ABC Firm mission and values, and reduces organizational risks. It has broad application throughout ABC Firm. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

SRT **–** Security Response Team

V. COORDINATOR / POLICY AUTHOR

Security & Compliance Officer

VI. AUTHORIZING OFFICER

Director

VII. EFFECTIVE DATE

INSERT DATE POLICY BECOMES ACTIVE

VIII. REVIEW DATE

Annual Review

IX. POLICY STATEMENTS

Security Event Program Organization

Computer Emergency Response Plans - ABC Firm management must prepare, periodically update, and regularly review emergency response plans that provide for the continued

operation of critical computer and communication systems in the event of an interruption or degradation of service.

Incident Response Plan Contents - The ABC Firm incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise including notification of relevant external partners. Specific areas covered in the plan include:

- Specific incident response procedures.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Identification and coverage for all critical system components.
- Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers.

Annual Incident Response Testing - At least once every year, the Information Security Department must utilize simulated incidents to mobilize and test.

Security Response Team

Security Response Team - Information Technology Department management must organize and maintain an in-house security response team (SRT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus infestations and hacker break-ins. A member of the Information Security Department is notified of any emergencies or incidents.

Computer Incident Response Team Availability - The ABC Firm Computer Emergency Response Team must be available at all times to respond to alerts that include but are not limited to evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.

Testing The Computer Emergency Response Team - At least once per year, the Information Security Department must utilize simulated incidents to mobilize and test the adequacy of the ABC Firm Computer Emergency Response Team.

Roles and Responsibilities

Incident Management Responsibilities - The individuals responsible for handling information systems security incidents must be clearly defined by the Information Security Manager. These individuals must be given the authority to define the procedures and methodologies that will be used to handle specific security incidents.

Designated Contact Person for all disasters and Security Events - Unless expressly recognized as an authorized spokesperson for ABC Firm, no worker may speak with the press or any other outside parties about the current status of a disaster, an emergency, or a security event that has been recently experienced.

Providing Information In Legal Proceedings - Employees are prohibited from providing any ABC Firm records, or any copies thereof, to third parties outside of ABC Firm or to government officials, whether in answer to a subpoena or otherwise, unless the prior permission of the President has first been obtained. Likewise, employees are prohibited from testifying to facts coming to their knowledge while performing in their official ABC Firm capacities, unless the prior permission of the President has first been obtained.

Program Communication

Display of Incident Reporting Contact Information - ABC Firm contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters and the intranet.

Incident Response and Recovery

Intrusion Response Procedures – **ABC-016 Incident Response Plan** outlines the procedures for intrusion response. The Information Security Department must document and periodically revise intrusion response procedures to keep up with the changing technology. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.

Information Security Problem Resolution - All information security problems must be handled with the involvement and cooperation of in-house information security staff, the ABC Firm Security Response Team, or others who have been authorized by ABC Firm.

Security Changes After System Compromise - Whenever a system has been compromised, or suspected of being compromised by an unauthorized party, System Administrators must immediately reload a trusted version of the operating system and all security-related software, and all recent changes to user and system privileges must be reviewed for unauthorized modifications.

Suspected System Intrusions - Whenever a system is suspected of compromise, the involved computer must be immediately removed from all networks, and predetermined procedures followed to ensure that the system is free of compromise before reconnecting it to the network.

Unauthorized Access Problems - Whenever unauthorized system access is suspected or known to be occurring, ABC Firm personnel must take immediate action to terminate the access of

Internal Investigations Information Confidentiality - Until charges are pressed or disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspected party.

Legal Proceeding Participation - Any ABC Firm worker called by a subpoena or in any other manner called to appear or testify before a judicial board or government agency must immediately notify the chief legal counsel in writing about the call.

Event Monitoring

Monitoring Event Logs - The usage of all ABC Firm shared computing resources employed for production activities must be continuously monitored and recorded. This usage history data must in turn be provided in real-time to those security alert systems designated by the Information Security Department (intrusion detection systems, virus detection systems, spam detection systems, etc.). When possible, all event logs will be shipped to a central logging system setup and retained per the **ABC-456 Disposal & Data Retention Policy**.

Intrusion Detection Systems - On all internal servers containing sensitive data, ABC Firm must establish and operate application system logs, intrusion detection systems, and other unauthorized activity detection mechanisms specified by the Information Security Department.

Reporting Information Security Events

Incident Reporting - All suspected information security incidents must be reported as quickly as possible through the approved ABC Firm internal channels.

Information Security Alert System - All ABC Firm employees are required to immediately inform the Information Security Department regarding any suspected information security problems.

Violation And Problem Reporting Protection - ABC Firm will protect employees who report in good faith what they believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other employees. Employees will not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation.

Violation And Problem Reporting Identity Protection - Employees who report to the Information Security Department a security problem, vulnerability, or an unethical condition within ABC Firm may, at their discretion, have their identity held in strict confidence. This means that the whistleblower's immediate supervisor, other members of the management team, as well as other ABC Firm employees who are not directly involved in the receipt of the report, will not be given the whistleblower's identity.

Events to Report

Off-Site Systems Damage And Loss - Employees must promptly report to their manager any damage to or loss of ABC Firm computer hardware, software, or information that has been entrusted to their care.

System Alerts and Warnings - Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Information Security Department. Users are prohibited from utilizing ABC Firm systems to forward such information to other users, whether the other users are internal or external to ABC Firm.

Unauthorized Activity - Users of ABC Firm information systems must immediately report to the Information Security Manager any unauthorized loss of, or changes to computerized production data. Any questionable usage of files, databases, or communications networks must likewise be immediately reported.

Unexpected Requests For Log-In Information - Other than the regular and expected ABC Firm log-in screens, users must be suspicious of all pop-up windows, web sites, instant messages, and other requests for a ABC Firm user ID and password. Users encountering these requests must refrain from providing their ABC Firm user ID and password, as well as promptly report the circumstances to the Help Desk.

Missing Access Devices - Identification badges and physical access cards that have been lost or stolen--or are suspected of being lost or stolen--must be reported to the Information Security Department immediately. Likewise, all computer or communication system access tokens (smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen--or are suspected of being lost or stolen--must be reported immediately.

Unintended Sensitive Information Disclosures - Unintended disclosures of sensitive ABC Firm information are serious matters, and they must all be immediately reported to both the Director of Client Services and the Information Security Manager. Such reporting must take place whenever such a disclosure is known to have taken place, or whenever there is a reasonable basis to believe that such a disclosure has taken place.

Software Malfunctions - All apparent software malfunctions must be immediately reported to the Information Security Manager. Security manager will document the malfunction with Connect-wise and contact the Director of Client Services.

Unauthorized Wireless Access Points - If an unauthorized wireless access point is detected on the ABC Firm network the Information Security Department must be notified.

Reporting to Third Parties

External Violation Reporting - Unless required by law or regulation to report information security violations to external authorities, management, in conjunction with representatives from the Information Security Department must weigh the pros and cons of external disclosure before reporting these violations.

Reporting Suspected Security Breaches To Third Parties - If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.

Loss Or Disclosure Of Sensitive Information - If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Information Security Department must be notified immediately.

System Vulnerability Exploitation And Victim Data - ABC Firm staff must not publicly disclose information about the individuals, organizations, or specific systems that have been damaged by computer crimes and computer abuses. Likewise, the specific methods used to exploit certain system vulnerabilities must not be disclosed publicly.

Vendor Vulnerability Disclosure - If a serious information system vulnerability is discovered by ABC Firm employees, and the vulnerability can be directly traced to a weakness in a certain vendor's hardware and/or software, then that vendor must promptly and confidentially be notified of the problem.

Contact with Authorities

Criminal Justice Community Contact - Technical information systems staff must not contact the police or other members of the criminal justice community about any information systems problems unless they have received permission from the Chief Executive Officer.

Law Enforcement Inquiries - Even if the requesting party alleges to be a member of the law enforcement community, ABC Firm employees must not reveal any internal ABC Firm information through any communications mechanism unless they have established the authenticity of the individual's identity and the legitimacy of the inquiry.

Contacting Law Enforcement - Every decision about the involvement of law enforcement with information security incidents or problems must be made by an ABC Firm senior partner. Likewise, every contact informing law enforcement about an information security incident or problem must be initiated by the Information Security Manager.

Requests To Cooperate In Investigations - ABC Firm employees must immediately report every request to participate in an information security investigation to the Chief Executive Officer. Any sort of cooperation with the requesting party is prohibited until such time that the President has determined that the participation is legal, is unlikely to cause problems for ABC Firm, and is requested by an authorized party.

Data Breach Management

Data Breach Response Plan Required - ABC Firm management must prepare, regularly review, and update a Data Breach Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.

Incident Review

Incident Response Plan Evolution - Lessons Learned - The incident response plan must be updated to reflect the lessons learned from actual incidents and developments in the industry.

Violation And Problem Analysis - An annual analysis of reported information security problems and violations must be prepared by the Information Security Department.

Collection of Evidence

Computer Crime Or Abuse Evidence - To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be immediately captured whenever a computer crime or abuse is suspected. The information to be immediately collected includes the current system configuration, all related event logs, as well as backup copies of all potentially involved files.

Evidence Storage -The relevant information for computer investigation must then be securely stored off-line until official custody is given to another authorized person or the President determines that ABC Firm will no longer need the information.

Sources Of Digital Evidence - For every production computer system, the Information Security Department must identify the sources of digital evidence that reasonably could be expected to be used in a court case. These sources of evidence must then be subject a standardized capture, retention, and destruction process comparable to that used for vital records.

Responsibility for Electronic Evidence Production - ABC Firm will appoint a single individual responsible for coordinating the discovery and presentation of electronic evidence that may be required to support litigation.

Information Classification - ABC Firm data that may be considered electronic evidence must be classified as CONFIDENTIAL and viewed only by authorized representatives or approved third parties involved in the investigation.

Investigation and Forensics

Computer Crime Investigation - Whenever evidence clearly shows that ABC Firm has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Extended Investigations - Extended investigations of security breaches must be performed while the suspected worker is given leave without pay. The reason for a suspect's leave without pay must not be disclosed to co-employees without the express permission of the President.

Forensic Analysis Data Protection - Every analysis or investigation using data storage media that contains information that might at some point become important evidence to a computer crime or computer abuse trial, must be performed with a copy rather than the original version. This will help to prevent unexpected modification to the original information.

Investigation Status Reports - The status of information security investigations must be communicated to management only by the lead investigator or the management representative of the investigation team.

Computer Crime Investigation Information - All evidence, ideas, and hypotheses about computer crimes experienced by ABC Firm, including possible attack methods and perpetrator intentions, must be communicated to the President and treated as restricted and legally privileged information.

Information Security Investigations - All ABC Firm internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the Information Security Manager.

Information Security Investigation Teams - Any person who personally knows the suspects, or who is friendly with them, for conflict of interest reasons is barred from participating on an information security incident investigation team.

Intrusion Investigations Details - Details about investigations of information system intrusions that may be still underway must not be sent via electronic mail. Likewise, to prevent such information from falling into the hands of intruders, files which describe an investigation now underway must not be stored on potentially compromised systems or anywhere on a related network where they could be reasonably expected to be viewed by intruders.

X. EXCEPTIONS

Exceptions to this policy will only be allowed with documentation and Director written approval. If any exception must be made, Director must approve.

XI. VIOLATIONS

Violations will be met with verbal or written acknowledgement of the violation. Director will determine if further action is to be taken.

Approved: _____ Date: _____

(Sam Smith)
(CEO)

XII. Document History			
Version	Date	Author	Comments
V1	5/13/2015	Mary Smith	Document Creation
V2	5/20/2015	Joe Johnson	Personnel Labels
V3	6/17/2015	Fred Roberts	Proof

Policy Title	Social Media Policy
Policy Number	ABC-567
Effective Date	INSERT DATE POLICY BECOMES ACTIVE
Responsible Office/Person	Security & Compliance Officer
Related Policies	ABC-001; ABC-006; ABC-022; ABC-011;

I. Contents

II. BACKGROUND

Social Media is a predominant part of popular culture. ABC Firm uses social media as means to advertise. How users act in an online manner is sensitive and this policy outlines policies that best reflect ABC Firm.

III. SCOPE

This policy applies to the entire ABC Firm team, including the President, Director, employees,

temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with ABC Firm, as well as volunteers and guests who have access to ABC Firm assets. Assets include but not limited to, workstations, servers, mobile phones, software, data, images or text owned, leased, or utilized by ABC Firm.

IV. DEFINITIONS

Policy – A policy is a governing set of principles that guide ABC Firm practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances the ABC Firm mission and values, and reduces organizational risks. It has broad application throughout ABC Firm. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

V. COORDINATOR / POLICY AUTHOR

Security & Compliance Officer

VI. AUTHORIZING OFFICER

Director

VII. EFFECTIVE DATE

(Determined by Director)

VIII. REVIEW DATE

Annual Review

IX. POLICY STATEMENTS

Company Assets - ABC Firm recognizes that employees may have personal accounts on Facebook, Linked-In, Twitter, Web-based email accounts such as Gmail, Hotmail and Yahoo. ABC Firm understands that employees may want to review those accounts during work days utilizing the company's electronic assets. It is approved to use social media on company assets only if necessary for company use.

Personal use - of social media should be reserved for break times and meal periods.

Social Media Privacy - ABC Firm users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to social media, this includes passwords, codes or other information that is entered on any company asset. **ABC-006 Acceptable Use Policy, ABC-022 Monitoring Policy,** and **ABC-011 Data Classification & Handling Policy** all outline strict rules for monitoring all data in and out of the network; this applies to all social media accessed from inside ABC Firm systems.

Social Media Slander - If you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or suppliers, or that might constitute harassment or bullying. ABC Firm expects all users to act in a morally exemplary manner wherever they may express themselves. Examples of in-appropriate conduct include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.

Sensitive Information on Social Media - Maintain the confidentiality of ABC Firm trade secrets and private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications on any social media or any other system not approved by the Security Department.

Company Opinions - Express only your personal opinions. Never represent yourself as a spokesperson for ABC Firm.

Social Media Advertising - ABC Firm may develop social media accounts for advertising purposes. Users may be asked to contribute to or maintain these accounts on behalf of the company. Only approved content may be posted to these social media accounts and the accounts may only be used for business purposes. The accounts, logins, passwords, information found on the accounts and any posts and/or submissions are the property of ABC Firm.

X. EXCEPTIONS

Exceptions to this policy will only be allowed with documentation and Director written approval.

XI. VIOLATIONS

Violations will be met with verbal or written acknowledgement of the violation. Director will determine if further action is to be taken.

Approved: _____ Date: _____
(Sam Smith)
(CEO)

XII. DOCUMENT HISTORY			
Version	Date	Author	Comments
V1	5/18/2015	Joe Smith	Document Creation
V2	5/22/2015	Fred Roberts	Personnel Labels
V3	6/17/2015	Sally Johnson	Proof

Policy Title	System Management Policy
Policy Number	ABC-789
Effective Date	INSERT DATE POLICY BECOMES ACTIVE
Responsible Office/Person	Security & Compliance Officer
Related Policies	ABC-987; ABC-456;

I. Contents

II. BACKGROUND

This policy defines the requirements for managing defaults configurations and changes to ABC Firm application, computer, and communications systems. This policy outlines access restrictions, session controls, authorization controls, awareness training, and vulnerability management.

III. SCOPE

This policy applies to the entire ABC Firm team, including the President, Director, employees, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with ABC Firm, as well as volunteers and guests who have access to ABC Firm assets. Assets include but not limited to, workstations, servers, mobile phones, software, data, images or text owned, leased, or utilized by ABC Firm.

IV. DEFINITIONS

Policy – A policy is a governing set of principles that guide ABC Firm practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances the ABC Firm mission and values, and reduces organizational risks. It has broad application throughout ABC Firm. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

V. COORDINATOR / POLICY AUTHOR

Security & Compliance Officer

VI. AUTHORIZING OFFICER

Director

VII. EFFECTIVE DATE

INSERT DATE POLICY BECOMES ACTIVE

VIII. REVIEW DATE

Annual Review

IX. POLICY STATEMENTS

Authorization

Production Operation Access Controls - All user-level and administrative-level access controls required by ABC Firm information security policies must be established and enabled before production information systems can be placed into operation.

Single Function Servers – Whenever possible, critical production servers should limit functionality to only one core network service (electronic mail, database server, web server, etc.). This will ensure down time is minimized.

Component Inventory – ABC Firm must maintain an inventory of all systems and related components that are under the scope of each system.

Configuration Controls

Baseline Standards – All information systems placed into product must conform to minimum security configurations standards defined by the Security Department.

Default Passwords - All vendor-supplied default passwords must be changed before any computer or communications system is used for ABC Firm business.

User ID Review - Before any production multi-user computer operating system is installed at ABC Firm, all privileged user IDs that are not assigned to a specific employee or partner must be renamed or disabled.

Unnecessary Software - Software features that could be used to compromise security, and that are clearly unnecessary in the ABC Firm computing environment, must be disabled at the time when software is installed on multi-user systems.

Unnecessary Functionality - All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed from the ABC Firm computer and communication infrastructure.

Remote Management

Access Encryption – All non-local access to ABC Firm systems must be encrypted using methods approved by the Security Department. All web-based access must use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Local Administration For Critical Systems – All ABC Firm critical product systems must be configured to only allow local administration.

Patches and Updates

Systems Administrators Install/Update Server Software - Only authorized Systems Administrators are permitted to install and/or update software on ABC Firm servers. See **ABC-987 Roles and Responsibilities Policy** for more instructions on who has access.

Software Patches, Bug Fixes, And Upgrades - All ABC Firm networked production systems must have an adequately-staffed process for expediently and regularly reviewing and installing all newly released systems software patches, bug fixes, and upgrades.

Security Patch Installation - All ABC Firm computer and communications system components and software must have the latest vendor-supplied security patches installed.

Critical Security Patch Installation Timing - All critical new security patches must be installed on ABC Firm computer and communications systems within one week.

Non-Critical Security Patch Installation, Fixes, And Upgrades - All non-critical security patches must be installed on ABC Firm computer and communications systems within one month.

Documenting Reasons Why Patches And Fixes Were Not Installed - If a patch or fix is not installed due to application conflicts or other incompatibilities, the involved Systems Administrator must document the reason and forward the documentation to the Security Department. These unpatched or unfixed vulnerabilities must be addressed and resolved to the satisfaction of the Security Manager during the next weekly information security review.

Third Party Applications - Executable programs provided by third party entities must be tested in accordance with Company policies and must also be properly documented before installation on any ABC Firm production system.

Vulnerability Management

Vulnerability Advisories - On a weekly or more frequent basis, the Security Department must review all information security vulnerability advisories issued by trusted organizations for items affecting ABC Firm systems.

Vulnerability Identification Software - To ensure that ABC Firm technical staff has taken appropriate preventive measures, all systems directly-connected to the Internet must be subjected to an automated risk analysis performed via vulnerability identification software at least once a month.

External Vulnerability Scans – Scan software to check all external facing vulnerabilities will be ran on ABC Firm systems once per month.

Internal Vulnerability Scans – Scan software to check all internal facing vulnerabilities will be ran on ABC Firm systems once per quarter or every 90 days.

Security Special Interest Groups - ABC Firm information security professionals must maintain memberships with security forums and professional associations to receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities.

System Security Status Tools - Every multi-user system must include sufficient automated tools to assist the Security Administrator in verifying the security status of the computer and must include mechanisms for the correction of security problems.

X. EXCEPTIONS

Exceptions to this policy will only be allowed with documentation and Director written approval.

XI. VIOLATIONS

Violations will be met with verbal or written acknowledgement of the violation. Director will determine if further action is to be taken.

Approved: _____ Date: _____

(Sam Smith)

(CEO)

XII. DOCUMENT HISTORY

Version	Date	Author	Comments
V1	5/18/2015	Mary Johnson	Document Creation
V2	5/22/2015	John Smith	Personnel Labels
V3	6/17/2015	Bob Roberts	Proof

Accellis Technology Group

Accellis Technology Group is one of the nation's leading providers of IT Consulting & Managed Services for the legal industry. We help law firms of all sizes reduce their day-to-day administrative tasks so they can focus on growing their business. Whether you need quicker access to help desk support, proactive IT management, improved security, or custom software solutions, Accellis can provide the expertise and direction to meet your goals.

This guide was developed by Accellis Technology Group based on years of field experience in the legal industry and is based on the ISO 27001 standards. Accellis Technology Group provides no warranties with respect to the guidance provided by this tool. Businesses should consult a cybersecurity expert before implementing any of the recommendations in this guide.

Additional resources:

- Law Firm Cyber Security Threat Matrix
- Avoid These Three Common Security Blind Spots
- Penetration Testing vs. Vulnerability Scanning
- Law Firm Cybersecurity: Practical Tips for Protecting Your Data
- Which type of hackers represent the biggest threat to law firms?
- The Biggest Cyber Security Threat to Law Firms is Not What You Think

Schedule a Free Consultation.

Accellis Technology Group helps simplify and streamline your cybersecurity and compliance efforts. We help you get in front of potential threats by ensuring your systems and policies are up-to-date with the today's latest industry standards and expectations.

Whether it's a security assessment, penetration test, or compliance evaluation – our team of certified security experts can ensure you're on the right track.

Schedule a Consultation

ACCELLIS
TECHNOLOGY GROUP