2008 Records Retention Guidelines

Compiled and Distributed by K2 Enterprises

www.K2e.com

Table of Contents

Records Retention Guidelines

This handout is distributed for attendees of our Paperless Office and Internal Controls seminars. The document has been compiled from multiple sources and represents a best practice approach to defining your corporate retention policy. Much of the information gathered herein is for the general benefit of the ready. It is collected from assumed knowledgeable sources. The authors make no claims on the value or legal standing of the information provided and recommends that in all cases that legal counsel be sought and received in writing when making decisions which could adversely affect the financial well being of the company.

If you have additional information you would like to provide to improve this documents for others or you find errors or omissions, please notify us immediately by contacting Dr. Bob Spencer at bob@k2e.com.

The retention and destruction of electronic records is critical to a business. There have been a number of court cases over the past few years where subpoenas revealed information from documents, both in paper and electronic form, which should have been destroyed. We have also had large fines where documents were destroyed where the company plainly had a fiscal responsibility to maintain the information. It is plan that we are not doing enough as managers of company assets to manage our data and that efforts in this area must be renewed.

Records Retention Policy

There are eight basic steps that can guide an organization in developing a sound record retention policy:

1. Evaluating statutory requirements, litigation obligations, and business needs;
2. Classifying types of records;
3. Determining retention periods and destruction practices;
4. Drafting and justifying record retention policy;
5. Training staff;
6. Auditing retention and destruction practices;
7. Reviewing policy periodically; and
8. Documenting policy, implementation, training, and audits.

We strongly recommend you seek legal counsel because the courts generally do not differentiate between what is hard copy form and that what is soft copy, or digital, form. The court will want the "best source" document submitted, and some documents, such as those we mentioned above which have a corporate or government seal on them should be maintained, but, if you keep your reports and other forms in electronic format, these should be admissible.

What is important is that you do have a formal written records retention policy. You are responsible for determining required, legislated retention periods based on your profession, industry, and state and federal laws.

The following is a suggested starting point and details which records must be kept permanently and which can be discarded after a time. The suggested retention time period generally begins at the end of the fiscal year in which the paper was created. For employment records, the schedule begins after the employee terminates. Items supporting your tax returns would be retained a minimum of three years after the applicable tax return was filed. Again, these are only guidelines to assist you in developing a suitable plan for your business.

Permanent Records

- Annual Financial Statements
- Articles of Incorporation
- Pension Records
- Company Stocks and Bonds
- Property Records, including account ledgers, appraisals, plan specifications, and sales
- Deeds
- Dividend Registers
- Tax Return (estate, gift, and income)
- General Ledgers
- Title Papers
- Contracts, Changes, and Specifications
- Audit Reports
- Union (Labor) Contracts
- Trademark Records
- Minutes of Meetings
- Warrants
- Note Registers
- Year End General Journal Entries

Ten Years

- Check Registers
- Personal Property Tax Returns
- Corporate Contacts
- Sales and Use Tax Returns
- Franchise Agreements
- Voucher Registers
- Accounting Journals
- Workers' Compensation Reports
- Tax Records

Seven Years

- Accident Reports
- Notes
- Bank Statements
- Options

- Checks
- Plant Acquisition Records
- Correspondence
- Property Damage Reports
- Depreciation Schedules
- Employee and Vendor Contracts
- Purchase Invoices
- Employment Applications and Contracts
- Sales Invoices, Slips, and Work Records
- Payroll Tax Returns
- Fixed Asset Records
- Social Security Tax Returns
- Inventory Records
- Uncollectible Accounts Records
- Invoices
- Vouchers
- Leases
- Equipment
- Withholding and Exemption Certificates
- Maintenance and Repair Records
- W-2 Forms
- Mortgage Records
- Personnel Files
- Paychecks
- Unemployment Claims

Five Years

- Bills of Lading
- Fire Damage Reports
- Cost Accounting Records
- Freight Draft, Bills, and Claims
- Daily Time Reports
- Shipping Tickets
- Sales Commission Reports
- Expense Reports

Three Years

- Bank Deposit Slips
- Insurance Policies (after expiration)
- Bank Reconciliations
- Petty Cash Records
- Budgets
- Purchase Order Copies

- Delivery Receipts
- Receiving Reports
- Remittance Statements
- Fidelity Bonds
- Requisitions
- Interim Financial Statements
- Surety Bonds
- Garnishments
- Travel Records

One Year

- Licenses (after expiration)

Retention Table

While the above list is great as a simple overview of the type of records which should be retained, the following table organizes these slightly different and includes specific items. Again, you should verify your retention policy against state and federal, or industry specific requirements.

TYPE OF RECORD	TIME PERIOD TO RETAIN
ACCOUNTING RECORDS	
Auditors' Report/Annual Financial Stmts.	Permanently
Bank Statements and Deposit Slips	7 Years
Cancelled Checks:	
- Fixed Assets	Permanently
- Taxes (Payroll Related)	7 Years
- Taxes (Income)	Permanently
- General	7 Years
- Payroll	7 Years
Cash Disbursements Journal	Permanently
Cash Receipts Journal	Permanently
Chart of Accounts	Permanently
Deeds, Mortgages, Bills of Sale	Permanently
Electronic Payment Records	7 Years
Employee Expense Reports	7 Years
Fixed Asset Records (Invoices, Cancelled Checks, Depreciation Schedules)	Permanently
Freight Bills and Bills of Lading	7 Years
General Journal	Permanently
General Ledger	Permanently
Inventory Listings and Tags	7 Years
Invoices: Sales to Customers/Credit Memos	7 Years
Patent/Trademark and Related Papers	Permanently
Payroll Journal	Permanently
Production and Sales Reports	7 Years
Purchases	7 Years
Purchase Journal	Permanently
Purchase Orders	7 Years
Sales or Work Orders	7 Years
Subsidiary Ledgers (Accts. Receivable, Accts. Payable, Equipment)	7 Years
Time Cards and Daily Time Reports	7 Years
Training Manuals	Permanently
Trial Balance - Year End	Permanently

EMPLOYEE BENEFIT PLAN RECORDS	
Actuarial Reports	Permanently
Allocation and Compliance Testing	7 Years
Brokerage/Trustee Statements Supporting Investments	7 Years
Financial Statements	Permanently
General Ledger and Journals	Permanently
Information Returns (Form 5500)	Permanently
Internal Revenue Service/Department of Labor Correspondence	Permanently
Participant Communications related to Distributions, Terminations, Beneficiaries	7 Years
Plan and Trust Agreements	Permanently

INSURANCE RECORDS	
Accident Reports and Settled Claims	6 Years after settlement
Fire Inspection and Safety Reports	7 Years
Insurance Policies (still in effect)	Permanently
Insurance Policies (expired)	7 Years

LEGAL DOCUMENTS	
Articles of Incorporation and Bylaws	Permanently
Buy-sell Agreements	Permanently
Contracts and Leases (still in effect)	Permanently
Contracts and Leases (expired)	7 Years
Employment Agreements	7 Years
Legal Correspondence	Permanently
Minutes	Permanently
Partnership Agreements	Permanently
Stock Certificates and Ledgers	Permanently

PERSONNEL RECORDS	
Child Labor Certificates and Notices	3 Years
Employment Application (from date of termination)	2 Years
Employment Eligibility Verification (I-9 Form) (from date of termination)	3 Years
Help Wanted Ads and Job Opening Notices	2 Years
Personnel Files (from date of termination)	4 Years
Records of job injuries causing loss of work	5 Years
Safety: chemical and toxic exposure records	30 Years
Union agreements and individual employee contacts (from date of termination)	3 Years

TAX RECORDS	
IRS or FTB Adjustments	Permanently
Payroll Tax Returns	4 Years
Property Basis Records	Permanently
Sales and Use Tax Returns	Permanently
Tax Returns and Cancelled Checks for Tax Payments	Permanently

Records Retention Tips

http://www.cpai.com/show-article?type=print&id=33

A formal records retention policy for engagement working papers and files is an important risk management tool. The policy should apply to all storage mediums, including paper, electronic files, e-mails, voicemail, and film. Once established by the firm, the records retention policy should be followed consistently and disclosed in engagement letters or other written communication to clients as it applies to the specific services to be rendered.

Consider the following issues when establishing a formal records retention policy:

Applicable statutes of limitation. The statutes for tort-based malpractice actions in more than one jurisdiction may be relevant, as many CPA firms or their clients do business in multiple states. In many jurisdictions, the "discovery rule" applies, meaning that the statute of limitations to file suit against a CPA begins to run on the date the client first knew or should have known of the act, error, or omission giving rise to the malpractice claim against the CPA.

Legal or regulatory requirements for CPAs. Despite the Supreme Court May, 2005 opinion that the U.S. Justice Department had overreached in prosecuting Arthur Andersen for shredding records pursuant to the firm's "document retention policy," destruction of documents that have been requested as part of a formal government investigation continues to be an offense under federal law, including, for example, the Sarbanes-Oxley Act of 2002 (SOX). A CPA firm should follow its record retention policy consistently so there will be no dispute as to the purpose of records destruction. In addition to SOX requirements, other federal, state, and local jurisdiction laws, rules, and regulations address document retention requirements, including those of state boards of accountancy. For example, the Public Company Accounting Oversight Board *Auditing Standard No. 3, Audit Documentation,* requires an auditor to retain audit documentation for seven years from report release date, and many state and municipal bodies in accordance with local statutes, require records be retained for specified periods by entities furnishing products and services.

Legal or regulatory requirements for clients. Some clients are subject to minimum periods of retention due to legal or regulatory requirements (e.g., entities receiving federal grants or funding). These client requirements may also impact CPA working paper retention requirements.

Client source documents. All client source documents used during an engagement and deemed necessary for retention in working papers should be copied and the originals should be returned to the client with a signed and dated letter. CPAs should not unintentionally assume the client's responsibility for maintaining client original records.

Financial statement services. Complete working paper files are critical in defending compilation, review, and audit engagements. Some files may need to be retained past the expiration of applicable statutes of limitations due to regulatory requirements, to respond to a tax audit or support conclusions included in later reports.

Tax services. Based on the discovery rule, claims relating to tax work may be alleged during a longer period of time. This is especially true for business tax clients and trust or estate work. CPAs should consider establishing different document retention policies for tax engagements based on the type of client and service rendered.

Consulting services. The discovery rule is also a significant issue in document retention policies for these practice areas. If the financial results from actions taken by the client in response to the consultant's recommendations are measured over many years (e.g., in employee benefit plans, financial plans, retirement plans, or estate plans), accountants should consider retaining related documents over an extended period. Alternatively, documentation on advice regarding short-range business issues, such as inventory management and accounts receivable collection, probably warrants a shorter retention period.

Legal and environmental issues. Clients may be involved in criminal or tort litigation or may be under investigation by regulators regarding legal or environmental issues that do not involve the firm. If the firm has received a subpoena in connection with these matters, CPAs must not destroy or alter the working papers even if the files are scheduled for destruction according to the firm's policy. Questions regarding these issues should be directed to legal counsel.

Current vs. former clients. CPAs should not base retention policies on client retention. An appropriately designed policy provides for timely destruction of documents no longer needed and avoids the need to distinguish between current and former clients.

The need to retain engagement working papers and files varies depending on laws and regulations applicable to the client and the state or other legal jurisdiction where services are rendered. Each firm should consult with legal counsel to develop a retention policy based on its particular situation and requirements. Additionally, firms should uniformly and consistently follow the policy and monitor its ongoing application as part of an overall quality control program.

Destruction of Records

Record retention policies are not just about retention. An effective retention policy allows for the routine destruction of certain records after a set period of time. The policy should set forth the retention time period as well as how the record will be destroyed once the time period has expired. So, how do you "destroy" your records once your policy's retention time period has expired?

Most associations will simply delete the information from the hard drive and consider it "destroyed." However, for the most part a deleted file is not, in fact, "destroyed." As most computer-savvy people know, it is virtually impossible to completely destroy an electronic document. The most common reason for this is the method in which computer operating systems delete files. Generally, an operating system renames the file and removes it from the computer's "directory." Then, it designates the physical space on the hard drive to be overwritten by new information. The problem is that most of the time, the physical space is not actually overwritten, thus the deleted file can be recovered. If it appears that electronic information may have been deleted, and it may be responsive to a document request or relevant in litigation, it is important to quickly bring in a qualified computer forensic specialist to retrieve the information and prevent any further destruction by overwriting with new information.

A recent study of used hard drives being sold on the internet found that 80 percent of the drives still had recoverable information. So, if you are going to dispose of a hard drive, you need to make sure that it's done correctly. Taking a hammer to the drive, or drilling a hole (or multiple holes) in it, is not likely enough to make the data unrecoverable. While it may make the hard drive inoperable, it rarely makes the data stored on the drive unrecoverable. Companies are now offering hard-drive shredding, which completely destroys the data on a hard drive; the end process involves completely melting all the particles within the drive. While inexpensive, the shredding is only an option if you can afford to constantly purchase new hard drives. Otherwise, you must find a way to delete the data, but allow for reuse of the drive.

Another option for destruction of media such as hard drives or backup tapes is "degaussing." Degaussing equipment is often used by the government to destroy its records. Data is stored in magnetic media, such as hard drives, tapes and diskettes (floppy disks), by making very small areas change their magnetic alignment to go in a certain direction. Degaussing equipment applies a strong magnetic field to the media, effectively destroying it because it removes the magnetic alignment. Again, this process is only useful if you can afford to continually purchase new storage media. Further, there is no way to be sure that the degaussing was successful. There is no log file created, so you cannot use this process if you must be compliant with certain federal regulations, such as the Health Insurance Portability and Accountability Act ("HIPAA") (related to personal medical information) or the Gramm-Leach-Bliley Act (relating to personal financial information), which specify how data destruction must occur and be tracked.

There are several commercial products for sale that will delete information stored on a hard drive so that it is not likely to be recoverable. These programs, often called "scrubbers," work by using a technique which deletes the data and then overwrites it with random data several times. The Defense Department recommends that the data be overwritten at least seven times before a drive

is discarded. However, the use of scrubbing software can be detected, so be sure there is no litigation hold in place and your retention policy allows for the destruction before commencing. Destruction may also be a problem when it involves corrupted media. For example, corrupt hard drives and backup tapes cannot be erased. Thus, shredding or degaussing is the only options for completely removing the information. When moving forward with information or media destruction, be sure to check as to whether the media can be truly erased, or whether it needs to be destroyed.

Once you have a policy in place that allows for the destruction of information, you need to be careful as to who does the actual destruction. Delegating the destruction of records may be a trap for the unwary, as it can appear to be a menial task that management may feel overqualified to perform (e.g., the shredding of documents). However, because most of the records contain sensitive information, or information that would be of value to competitors, having upper management or a specialized outside company perform the destruction generally is recommended. Non-management employees often have an economic incentive to maintain the information, rather than destroy it, as is evident by the numerous lawsuits involving theft of trade secrets by companies against former employees.

E-discovery Amendments to the Federal Rules of Civil Procedure December, 2006

One of the most driving issues to going Paperless is to improve an organizations ability to manage information. Yet many organizations are truly unaware of how to manage such data electronically and what laws exist that governs the storage, retrieval and retention of such information electronically. In December 2006 the Federal Rules of Civil Procedure were amended to specifically address e-discovery. Business owners should make themselves aware of these changes as appropriate. The Amendments to the Federal Rules of Civil Procedure may be found at http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. The following is a refined definition of the 60 plus pages and the Rules they apply to.

The e-discovery amendments originated with the Advisory Committee on Civil Rules, which first heard about problems with computer-based discovery in 1996 and began intensive work on the subject in 2000. The Advisory Committee considered numerous alternatives, perspectives, and ideas in determining whether amendments specifically addressing electronic discovery were necessary, and, if so, what the language of any such amendments should be. In August 2004, the Committee published its proposed amendments. Following the public comment period – during which over 250 individuals and organizations provided feedback – the Advisory Committee made several additional modifications, resulting in the final package of amendments that was ultimately approved by the Judicial Conference and the United States Supreme Court.

The amendments cover five related areas, which are described in more detail below:

(a) definition of discoverable material;
(b) early attention to issues relating to electronic discovery, including the format of production;
(c) discovery of electronically stored information from sources that are not reasonably accessible;
(d) the procedure for asserting claim of privilege or work product protection after production; and
(e) a "safe harbor" limit on sanctions under Rule 37 for the loss of electronically stored information as a result of the routine operation of computer systems.

In addition, amendments to Rule 45 correspond to the proposed changes in Rules 26-37.

1. Definition of Discoverable Material

The amendments introduce the phrase "electronically stored information" to Rules 26(a) (1), 33, and 34, to acknowledge that electronically stored information is discoverable. The expansive phrase is meant to include any type of information that can be stored electronically. It is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and technological developments.

2. Early Attention to Electronic Discovery Issues

Several of the amendments require the parties to address electronically stored information early in the discovery process, recognizing that such early attention is crucial in order to control the scope and expense of electronic discovery, and avoid discovery disputes. Rule 26(a) (1) (B) adds electronically stored information to the list of items to be included in a party's initial disclosures. Rule 16(b) (5) adds provisions for the disclosure or discovery of electronically stored information as an item that may appropriately be included in the court's scheduling order. Rule 26(f) expands the list of issues that must be discussed as a part of the meet and confer process, and includes a requirement that parties develop a discovery plan that addresses issues relating to the discovery of electronically stored information – including the form or forms in which it will be produced. It also requires parties to discuss any issues relating to the preservation of discoverable information, and address issues relating to claims of privilege or work product protection.

3. Format of Production

An amendment to Rule 34(b) addresses the format of production of electronically stored information, and permits the requesting party to designate the form or forms in which it wants electronically stored information produced. The rule does not require the requesting party to choose a form of production, however, since a party may not have a preference or may not know what form the producing party uses to maintain its electronically stored information. The rule also provides a framework for resolving disputes over the form of production, in the event that the responding party objects to the requested format(s). Finally, the rule provides that if a request does not specify a form of production, or if the responding party objects to the requested form(s), the responding party must notify the requesting party of the form in which they intend to produce the electronically stored material – with the option of producing either (1) in a form in which the information is ordinarily maintained, or (2) in a reasonably usable form.

4. Electronically Stored Information from Sources that Are Not Reasonably Accessible

Amended Rule 26(b) (2) creates a two-tiered approach to the production of electronically stored information, making a distinction between that which is reasonably accessible, and that which is not. Under the new rule, a responding party need not produce electronically stored information from sources that it identifies as not reasonably accessible because of undue burden or cost. If the requesting party moves to compel discovery of such information, the responding party must show that the information is not reasonably accessible because of undue burden or cost. Once that showing is made, a court may order discovery only for good cause, subject to the provisions of the current Rule 26(b) (2) (i), (ii), and (iii). *

This two-tier system seeks to provide a balanced, equitable approach to resolve the unique problem presented by electronic stored information which is often located in a variety of locations of varying accessibility – strongly favoring the production of relevant information from more easily accessible sources where possible. This provision received a great deal of attention during the public comment period, and the Advisory Committee made substantial changes to both the proposed rule and to the accompanying notes to address the concerns voiced, and to

balance the interests of both requesting and responding parties. The responding party receives protection from being forced to tap hard-to-access sources, where retrieving information or determining the presence of responsive content cannot be achieved without incurring substantial burden or cost. The requesting party benefits from knowing the sources the responding party does not intend to search, and has a method of obtaining this information if it is truly warranted.

5. Asserting Claim of Privilege or Work Product Protection After Production

The addition to Rule 26(b) (5) sets forth a procedure through which a party who has inadvertently produced trial preparation material or privileged information may nonetheless assert a protective claim as to that material. The rule provides that once the party seeking to establish the privilege or work product claim notifies the receiving parties of the claim and the grounds for it, the receiving parties must return, sequester, or destroy the specified information. The Committee Note clearly states that the rule does not address whether the privilege or protection was waived by the production, but simply prohibits the receiving party from using or disclosing the information, and requires the producing party to preserve the information, until the claim is resolved.

6. "Safe Harbor"

Much of the commentary received during the public comment period on the e-discovery amendments focused on the Rule 37(f) safe harbor provision. This rule provides that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system. It responds to the routine modification, overwriting, and deletion of information that attends the normal use of electronic information systems.

The Advisory Committee notes that the "routine operation of an electronic information system" refers to the ways in which such systems are generally designed and programmed to meet the party's technical and business needs, and includes the alteration and overwriting of information that often takes place without the operator's specific direction or awareness. The Committee further observes that such features are "essential to the operation of electronic information systems," and that there is "no direct counterpart in hard-copy documents."

The protection of Rule 37(f) applies only to information lost due to the routine operation of an information system, and only if such operation was in good faith. The Committee Note discusses the effect that the existence of a preservation obligation may play in determining whether or not the operation was in good faith, and expressly cautions: "A party cannot exploit the routine operation of an information system to evade discovery obligations by failing to prevent destruction of stored information that it is required to preserve."

SAMPLE RECORD RETENTION POLICY

Objective

This comprehensive record retention policy balances the benefits of retaining records that materially support professional reports or advice, or permit an acceptable level of client service, against the substantial costs of storing and retrieving.

Definitions

Engagement Records are all records that are relevant to and materially support the Firm's professional opinions, advice or work product. This includes workpapers, reports or documents transmitted by the Firm, and records or documents received by the Firm, which are material to the execution of our client engagements. For existing clients only, Engagement Records included in permanent files are retained and updated annually and, as a result, are not subject to the retention period. Engagement Records do not include administrative records, such as billing records.

Engagement Records include electronic files in the possession of the Firm's personnel that are relevant to the Firm's professional opinions, advice or work product. Electronic files include E-Mail transmissions, client files or E-Mail messages contained on a professional's computer hard drive and client files maintained on network file servers.

Client Records are documents in the Firm's possession, which ordinarily should be kept and maintained by the client. Examples of Client Records include depreciation and amortization schedules, schedules supporting and actual journal, closing or reclassification entries, asset basis information, etc. A Client Record does not include any workpaper developed by the Firm or prepared by client personnel at the Firm's request which workpaper is integral to the performance of a client engagement.

Applicability

This Policy applies to Engagement Records and Client Records obtained, developed or relied upon in connection with:

- Compilation, review, audit, prospective financial presentation, and other agreed-upon procedures, special reports or attestation engagements,
- The preparation and/or filing of tax returns or the performance of tax planning, tax advice, or tax representation,
- Engagement Records obtained or developed in connection with consulting services engagements, and
- Any other engagement records arising out of all professional services or work product.

Policy

Engagement Records Retention Period - Engagement Records for all professional services shall be retained for a period of seven years from the year end of client or the date of the Firm's last planning, advice, consultation or representation engagement for such client. If there is any ambiguity regarding

the date for implementation of retention, all doubts shall be resolved in favor of the earliest implementation date. See **Exhibit A** for a summary of retention periods related to Engagement Records.

Exception - A longer retention may be deployed in specific cases to the extent required by any applicable law, regulation or engagement contract. It is contemplated that the instances of required retention beyond seven years will be infrequent and unusual.

To the extent that the Engagement Records are relevant to any pending tax examination, civil litigation or regulatory proceeding, the applicable retention period shall be extended for a period of time reasonably necessary to facilitate disposition of the examination, litigation or proceeding.

Following the initial retention period specified above, the Manager in Charge (MIC), or his designee, shall cause the Firm to no longer retain any Engagement Records (See "Method of Disposal of Client or Engagement Records").

Client requests that Engagement Records should be retained for a period longer than the prescribed period shall be pre-approved in writing by the Firm's Presiding Member.

Under certain circumstances, the Firm's Legal Counsel may direct the MIC to retain Engagement Records for a designated period of time.

Retention of Client Records - The original (or copy, if appropriate) Client Records should preferably be returned to the client at the end of the engagement. To the extent Client Records have not been returned to the client, Client Records shall be retained for a period of seven years. However, Client Records need not be retained if at the end of the engagement (or termination date); a representation is obtained from the client indicating that such records are no longer needed by the client. Careful consideration must always be exercised to assure that Client Records, which are being returned to or copied for the client or consultant, does not include descriptions of our procedures or conclusions.

Successor Auditor/Accountant - We will normally not allow a review of our workpapers until the fees for all professional services rendered have been paid. Additionally, we must receive (a) notification that the successor has been appointed by our former client, (b) written authorization by our former client, and (c) a written letter of acknowledgment by the successor auditor. In the absence of unusual circumstances, we will make certain workpapers (e.g. those workpapers that are related to matters of continuing significance) available for review in our office by the successor auditor or accountant. Our workpapers should remain under our control at all times.

Continuing significance includes workpapers such as: the analysis of accounts, report grouping support, internal control structure understanding documentation, summary of proposed audit adjustments, information regarding key audit issues, tax workpapers pertinent to accurate completion of subsequent year tax returns, such as LIFO inventory computations, tax only depreciation computations and carry forward schedules relative to accounting method and period revisions.

Continuing significance does not include the following and they should not be made available to successor auditor: the risk assessment and overall audit plan, audit program sheets, tax research notes or memorandum, or administrative materials such as billing or time records.

We should make a separate copy for our files of any document which has been copied and transmitted to the successor auditor/accountant. This is to avoid problems and issues regarding the exact nature and extent of documents given to the successor.

Successor Consultant - On consulting engagements, a successor consultant shall not be permitted to review or copy Engagement Records.

Method of Disposal of "Client" or "Engagement" Records - Client Records or Engagement Records that are not required to be retained should be disposed of in a manner that assures the confidentiality of the information contained therein. This typically entails the shredding of the materials while under Firm control.

Firm Administrative Records for Retention – The Firm also needs to maintain certain administrative records for purposes as required by law and internal operational purposes. A schedule of records and the related retention periods is identified in Exhibit A. Under no circumstances should any administrative record not identified in Exhibit A be maintained for more than seven (7) years unless approved by the Presiding Member or Executive Director.

Exception to the Policy - Exceptions to this Policy shall be pre-approved by the Firm's Legal Counsel.

Effective Date: This Policy shall be effective immediately.

Exhibit A – Record Retention Guidelines

Description of records	Paper	Electronic
Personnel Records		
Personnel File contents	Indefinite	N/A
Applications, resumes for non hires	1 Year	N/A
Job progress evaluations	After annual evaluation is completed	N/A
Annual Evaluations	3 Years	3 Years
Personnel Policy - Annual summary	10 Years	N/A
Payroll Records		
Annual Payroll information	7 Years	7 Years
Interim Payroll information	3 Years	3 Years
PTO request forms/summary records	3 Years	3 Years
Payroll Tax Returns	4 Years	4 Years
Administrative Files		
Work Orders/Tax Tickets	7 Years	N/A
Member and Staff Correspondence-Admin.	3 Years	5 Years
Time Records and Time Books	1 Year	5 Years
Expense Reports	4 Years	4 Years
CPE records		
Annual Reports with Attendance	5 Years	N/A

In house Course materials	5 Years	N/A
CPE course books & materials	5 years	N/A
Purchase orders	3 years	3 Years
Invoices	4 Years	N/A
Canceled checks	4 Years	N/A
General Ledgers – Annual	Indefinite	Indefinite
Firm Financial Reports		
Monthly	4 Years	4 Years
Annual	Indefinite	Indefinite
Partnership/PLLC Tax Returns and supporting	Indefinite	Indefinite
W/Ps		
Minutes	Indefinite	3 Years
Contracts - current	Indefinite	N/A
Contracts – Expired	4 Years	N/A
Depreciation Schedules – Year End	Indefinite	Indefinite
New Client Sheets	3 Years	N/A
Lost Client Sheets	7 Years	N/A
Client Change Sheets	3 Years	N/A

Description of records	Paper	Electronic
Client Records		
Engagement Records – Current & Former Clients		
Audit File work papers	7 Years	7 Years
Tax Return work papers	7 Years	7 Years
Compilation work papers	7 Years	7 Years
Review Work papers	7 Years	7 Years
Agreed Upon procedures	7 Years	7 Years
Special Reports/Attestation engagements	7 Years	7 Years
Consulting Services	7 Years	7 Years
Permanent Files		
Current Client	Indefinite	Indefinite
Former Client	7 Years	7 Years
Contents of Permanent File (NLC's - 7 Years)		
Client Correspondence	7 Years	7 Years
Financial Statements	7 Years	Indefinite
Tax Returns & related correspondence	Indefinite	Indefinite
Forms, Schedules, computations, other contents	Indefinite until replaced then file with current year work papers	After replaced retain for 7 Years

Exhibit B – Email Policy

The purpose of this policy is to ensure the proper use of the firm's email system and make users aware of what the firm deems as acceptable and unacceptable use of its email system. The firm reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

Legal Risks

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- If you send emails with any libelous, defamatory, offensive, racist or obscene remarks, you and the firm can be held liable.
- If you forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you and the firm can be held liable.
- If you unlawfully forward confidential information, you and the firm can be held liable.
- If you unlawfully forward or copy messages without permission, you and the firm can be held liable for copyright infringement.
- If you send an attachment that contains a virus, you and the firm can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, the user will be fully liable and the firm will disassociate itself from the user as far as legally possible.

Legal Requirements

The following rules should be adhered to. It is prohibited to:

- Send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.
- Forge or attempt to forge email messages.
- Disguise or attempt to disguise your identity when sending mail.
- Send email messages using another person's email account.

Best Practices
The firm considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good client service. Users should take the same care in drafting an email as they would for any other communication. Therefore the firm wishes users to adhere to the following guidelines:

Writing emails:

- Write well-structured emails and use short, descriptive subjects.

- The firm's email style is informal. This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations and characters such as smileys however, is not encouraged.

- Signatures should include your name, job title and company name. A disclaimer will be added underneath your signature (see Disclaimer)

- Users must spell check all mails prior to transmission.

- Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.

- Do not write emails in capitals.

- If you forward mails, state clearly what action you expect the recipient to take.

- Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).

- Only mark emails as important if they really are important.

Replying to emails:

- Emails should be answered promptly within at least 8 working hours, but users should endeavor to answer priority emails within 4 hours.

- Never respond to email in anger or haste. Consider responses carefully, even hold the reply in the Draft folder while considering if the response is appropriate.

- Priority emails are emails from existing customers and business partners.

Maintenance:

- Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.

- Message that are to be retained for an extended period should be managed via a network server, or moved from your local email folder and stored in the customer, project or engagement and archived with other project related files until the retention period has been satisfied.

Personal Usage
Although the company's email system is meant for business use, the firm allows personal usage if it is reasonable and does not interfere with work. However, the sending of chain letters, junk mail, jokes and executables is prohibited. All messages distributed via the company's email system are the firm's property.

Confidential Information
Never send any confidential information via email. If you are in doubt as to whether to send certain information via email, check this with your supervisor first.

Passwords
The use of passwords to gain access to the computer system or to secure specific files does not provide users with an expectation of privacy in the respective system or document.

Email Retention
All emails will be deleted after 120 days. If a user has sufficient reason to keep a copy of an email, the message must be saved to the appropriate folder in the firm document management system. Users are not permitted to archive messages to local hard drives.

Email Accounts
All email accounts maintained on our email systems are property of the firm. Passwords should not be given to other people. Email accounts not used for 60 days will be deactivated and possibly deleted.

System Monitoring
Users expressly waive any right of privacy in anything they create, store, send or receive on the company's computer system. The firm can, but is not obliged to, monitor emails without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, the firm reserves the right to take disciplinary action, including termination and/or legal action.

Disclaimer
The following disclaimer will be added to each outgoing email:

The contents of this email transmission, including any documents transmitted by or accompanying this email transmission, contain confidential information, belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. This email and its content may not be forwarded to any other recipient except as authorized by law.

Finally, the recipient should check this email and any attachments for the presence of viruses. The firm accepts no liability for any damage caused by any virus transmitted by this email.

Additional disclaimer information may be required based on department or industry regulations.

Questions

If you have any questions or comments about this Email Policy, please contact the HR Director. If you do not have any questions the firm presumes that you understand and are aware of the rules and guidelines in this Email Policy and will adhere to them.

Declaration

I have read, understand and acknowledge receipt of the Email policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

Signature: _____

Date: _____

Printed Name: _____

Exhibit C – SEC Client Record Retention

Retention of Memoranda, Correspondence, Communications and Other Documents and Records

1) SEC Rule 2-06 of Regulation S-X specifies retention requirements for:

    i) Workpapers and other documents that form the basis of an audit or review (workpapers); and

    ii) Memoranda, correspondence, communications, other documents and records (other records), which:

        (1) Are created, sent or received in connection with an audit or review, and

        (2) Contain conclusions, opinions, analyses, or financial data related to the audit or review.

2) Workpapers are defined in Rule 2-06 as documentation of auditing or review procedures applied, evidence obtained and conclusions reached by the Firm in the audit or review engagement, as required by auditing or review standards established or adopted by the SEC or the Public Company Accounting Oversight Board (PCAOB). PCAOB Auditing Standard No. 3, Audit Documentation, establishes general requirements of documentation the auditor should prepare and retain in connection with engagements conducted pursuant to PCAOB standards. Workpapers should contain sufficient documentation to meet the standards established by all applicable professional standards.

3) When consulting in writing with persons outside of the engagement team, a Record of Consultation should be made. You should also follow the Firm's policies for resolving and documenting the resolution of differences of opinion between members of the engagement team or between members of the engagement team and a reviewer or consultant. A Record of Consultation setting forth the issue and its resolution should be prepared for all differences of opinion that could not be resolved at the engagement team level.

4) Other records should be retained if they support the Firm's final conclusions regarding the audit or review, or contain information or data relating to a significant matter, that is inconsistent with the Firm's final conclusions regarding that matter or the audit or review. However, other records do not include items such as:

    a) Superseded drafts of memoranda, financial statements or regulatory filings;

    b) Notes on superseded drafts of memoranda, financial statements or regulatory filings that reflect incomplete or preliminary thinking;

    c) Previous copies of workpapers that have been corrected for typographical errors or errors due to training of new employees;

    d) Duplicates of documents; or

    e) Voice mail messages.

The following record retention policies are effective for any workpapers or other records connected with an SEC client that meets the record retention criteria of Rule 2-06.

1) In compliance with Regulation S-X and related professional standards, the Firm will retain, for a period of seven years from the date we grant permission to use the auditor's report in connection with the filing of the initial annual report including the financial statements encompassing the period covered by such audit or review (report release date), the audit or review documentation (working papers), and all memoranda, correspondence, communications, other documents, and records, including electronic records (other records) that:

    a) Are created, sent or received in connection with the audit or review, and

    b) Contain conclusions, opinions, analyses, or financial data related to the audit or review.

2) All other records subject to this policy will be retained in the media in which they were sent or received (or, if not sent or received, in the media in which they were created).

3) The following files should be used to retain the working papers and other records:

    a) An electronic (paperless) annual working paper database;

    b) An electronic (paperless) quarterly review working paper database;

    c) An electronic client correspondence database;

    d) A paper current file; and

    e) A permanent file.

4) Concurrently with the filing of the initial annual report including the financial statements encompassing the period covered by the Firm's audits and reviews:

    a) All electronic databases related to that period should be locked down;

    b) After lock down, all electronic databases should be rolled forward and paper current files should be created to allow for the continuing retention of other records;

    c) No workpapers should be deleted from the paper files; and

    d) All subsequent additions to or alterations of the paper current file should indicate the date of the addition or alteration, the name of the person who prepared the addition or alteration, and the reason for the addition or alteration.

5) E-mail messages created, sent or received by members of the Firm that meet the retention criteria must be retained for the seven-year period. In order to comply with this requirement, the Firm has established a separate correspondence database for each SEC engagement created in the EA Creation database. Each correspondence database has been assigned its own e-mail address. For e-mail messages created or sent by Firm personnel, the sender is responsible for including this separate e-mail address on all messages meeting the retention criteria. For external e-mail messages received by Firm personnel, the recipient is responsible for forwarding all messages meeting the retention criteria to the separate e-mail address.

E-mail messages sent or received from a computer that operates on a system outside the Firm cannot be sent directly to the correspondence database. Consequently, a member who sends or receives a message that meets the retention criteria from a computer that operates on a system outside of the Firm, is responsible for forwarding such message to his or her own firm e-mailbox and, subsequently, to the correspondence database.

Other records sent to the correspondence database may be deleted. However upon deletion, a reason for the deletion must be indicated. All deleted items will be stored in a separate view of the database and will not be permanently removed from the database until lockdown. Prior to lockdown the engagement Member is responsible for reviewing the items in the deletions view for propriety. The only appropriate reasons for deletion of another record are: it is 1) a superseded draft 2) a duplicate item or 3) an incomplete or preliminary communication.

6) If a report is not issued in connection with an engagement, the electronic databases should be locked down on the date that fieldwork was substantially completed and the audit documentation must be retained for seven years from the date that fieldwork was substantially completed. If we were unable to complete the engagement, then the electronic databases should be locked down on the date the engagement ceased and the audit documentation must be retained for seven years from the date the engagement ceased.

7) Audit documentation must be retained for a longer period of time if required by law.

SEC Client Record Retention Q & A

1) How should we monitor that all correspondence that should be retained has been retained?

   There is no way, within the system, to track whether or not correspondence that should have been copied into the Correspondence database was not. The responsibility for making sure we are following the requirements of Rule 2-06 rests with the engagement team.

2) SEC Rule 2-06 states "other records should be retained whether they support the Firm's final conclusions regarding the audit or review, or contain information or data relating to a significant matter, that is inconsistent with the Firm's final conclusions regarding that matter or the audit or review." How is the term "significant" defined?

   The determination of whether a matter is insignificant has been left to the discretion of the engagement team. In addition to significant audit findings or issues (see M&P MCAP Section 830.00) there may be other matters that in the professional judgment of the engagement team are significant.

3) If a paperless database was rolled forward/set up before the update that created the correspondence databases will the Correspondence database be created automatically or do I need to create a new paperless database?

   The Correspondence database will be created automatically, but you will need to go back into the EA creation database and click the Add Server Icons button to access it.

4) Will all individuals who have access to the workpaper database automatically have access to the Correspondence database?

   Yes, the Correspondence database is created using the same access control list as the paperless workpaper database.

5) What about an individual who performs services to the SEC client, but is not listed as an owner/member of the engagement team in the EA creation database? Can these individuals send messages to the Correspondence database?

   Yes, anyone can forward a message to the Correspondence database; however only individuals listed in the EA creation client document will be able to view the message from within the Correspondence database.

6) Does this policy apply to FDICIA banks?

   Only to those who are also "issuers"

7) Do TS and CS members of the client service team need to comply with this policy?

   If TS or CS personnel create, send or receive workpapers or other records that would meet the record retention criteria of Rule 2-06 they need to comply with this policy.

8) If a tax professional sends e-mail to an SEC client on a matter unrelated to the audit or review must that e-mail be retained?

   If the message contains no information relevant to the audit or review it does not need to be retained.

9) If we lock down the quarterly databases after each 10-Q is issued what should we do with correspondence during the period between engagements?

   Once the quarterly database is locked down, it should immediately be rolled forward so a new correspondence database is created, thereby allowing for ongoing retention of other records.

10) Do you have to retain the same information in both the 10-K and 10-Q databases?

    No, information only needs to be retained in one place.

11) If a client sends e-mail that meets the criteria for retention to a member of the engagement team, does it need to be forwarded manually to the Correspondence database or can the client send it directly to the database?

    The e-mail addresses of the Correspondence databases are not available outside the firm. Any messages sent from the outside (e.g., from clients or a personal e-mail address) will need to be forwarded to the Correspondence database from within the Firm's e-mail system.

12) If you have documented in the paperless workpaper file information received in e-mail, can you delete the e-mail?

    If you have copied and pasted the entire e-mail message into the paperless workpapers then yes you may delete the e-mail. Otherwise, you should send the e-mail to the correspondence database.

13) Can we edit e-mail messages once they are in the correspondence database?

    It is physically possible to edit the messages; however this is something that should not be done.

14) Can we use a client folder on the network to save all of these documents instead?

    No, files copied to the network are not subject to the record retention process so workpaper/ other records should not be stored there.

15) If we have a folder on the network where we store workpaper/other records should we delete it?

    Yes

16) What about Paperless workpaper files, can we keep those on the network?

    Provided a copy of the Paperless workpaper files are included in the paperless database, the Paperless workpaper files may still be maintained on the network.

Recommended Guidelines For RETAINING RECORDS

Making decisions on retaining files is not always an easy task. Our professionals are providing you with the recommended guidelines for retaining both paper & electronic records.

ACCOUNTING

Accounts payable ledgers and schedules *7 years*
Accounts receivable ledgers and schedules *7 years*
Audit reports of accountants *Indefinitely*
Budgets *3 years*
Cash receipts records *7 years*
Charts of accounts *Indefinitely*
Check register and cash books *Indefinitely*
Depreciation schedules *Indefinitely*
Expenses analyses and expense distribution schedules 2 years
Financial statements (end-of-year) *Indefinitely*
General and private ledgers (and end-of-year trial balances) *Indefinitely*
Internal audit reports 5 years
Internal reports (misc.) *3 years*
Invoices from vendors *7 years*
Invoices to customers *7 years*
Journals *Indefinitely*
Low-income housing records *7 years*
Notes receivable ledger and schedules *7 years*
Petty cash vouchers *3 years*
Plant cost ledgers *7 years*
Purchase orders (except purchasing department copy) *1 year*
Purchase orders (purchasing department copy) *7 years*
Requisitions *1 year*
Sales records *7 years*
Subsidiary ledgers *7 years*
Tax returns, work papers and revenue agents' reports *Indefinitely*
Voucher register and schedule *7 years*
Vouchers for payments to vendors *7 years*

BANK

Bank deposits *4 years*
Bank reconciliations *1 year*
Bank statements *7 years*
Canceled checks (daily payments *7 years*
Canceled checks (major payments, ie, taxes, purchases of property, special contracts, etc.) *Indefinitely*
Duplicate deposit slips *1 year*

COMPUTERIZED RECORDS

Records must be maintained in a retrievable format according to these time guidelines. Additionally, documentation describing the application, procedures and controls utilized, as well as detail information for the records must be available.

DOCUMENTATION

Contracts and leases (expired) *7 years*
Contracts and leases (still in effect) *Indefinitely*
Deeds, mortgages, and bills of sale *Indefinitely*
Inherited property valuations *Indefinitely*
Partnership agreements *Indefinitely*
Property appraisals *Indefinitely*
Property records (including costs, depreciation reserves, end-of-year trial balances, depreciation schedules, blueprints and plans) *Indefinitely*
Real estate records *Indefinitely*
Trademark registrations *Indefinitely*

EMPLOYEE

Employee benefit plan records *7 years*
Employee personnel records (after termination) *4 years*
Employment applications *3 years*
Payroll and payroll tax records *7 years*
Retirement and pension records *Indefinitely*
Savings bond registration records of employees *3 years*
Time records *7 years*
Vouchers for payments to employees (including travel and entertainment) *7 years*

INSURANCE

Accident reports and claims (completed) *7 years*
Insurance policies (expired) *3 years +*
Insurance records, open or unresolved accident reports, claims, policies, etc. *Indefinitely*

INVENTORY

Inventories of products, materials, and supplies *7 years*
LIFO inventory detail information *7 years to Indefinitely*
Physical inventory tags *3 years*
Receiving sheets *1 year*
Scrap and salvage records (inventories, sales, etc.) *7 years*
Stockroom withdrawal forms *1 year*

MISCELLANEOUS

Correspondence (general) *3 years*
Correspondence on legal, tax and major matters *Indefinitely*

STOCK

Capital stock and bond records; ledgers, transfer registers, stubs showing issues, records of interest coupons, options, etc. *Indefinitely*
Minute books of directors and stockholders including by-laws and charter, certificate of incorporation *Indefinitely*
Options records (expired) *7 years*
Stock & bond certificates (canceled) *7 years*

Certified Public Accountants
Business & Management Consultants
