RECORD RETENTION

*Record Retention and Destruction Policy*

[**Note:** The policy template should be modified as appropriate to reflect the firm's specific factual situation. The firm is also urged to consult with legal counsel and the applicable state board(s) of accountancy to ensure adequate compliance with applicable laws.]

<Firm Name> recognizes that the firm's engagement and administrative files are critical assets. As such, the firm has established this formal written policy for record retention and destruction in accordance with applicable state and federal laws. Compliance with this policy is mandatory for all employees.

**Engagement Files**

Engagement files are defined, for purposes of this policy, as all records related to the engagement, including workpapers and other documents that form the basis of the services rendered by the firm. They include, but are not limited to, all documentation reflecting the procedures applied, evidence obtained, and conclusions reached in the audit, review, compilation, or preparation of financial statements; or applicable workpapers/work products that support any tax, consulting, or other engagements. In order to adequately address the needs of the firm and meet the current requirements established by the profession and the regulatory agencies, this policy will address separately the document retention requirements for engagement files by the categories indicated below.

**Audit/Review/Compilation/Preparation Services**

<Firm Name> will retain all records related to the audit, review, compilation or preparation (including electronic records) for a period of <number (not to be less than seven)> years from the conclusion of the audit, review, compilation, or preparation that meet the following ***two criteria:***

**1. *The records have been created, sent, or received in connection with the audit, review, compilation, or preparation;***

**and**

**2. *The records contain conclusions, opinions, analyses, and/or financial data related to the audit, review, compilation, or preparation, or significant information that is inconsistent with the final conclusions, opinions, or analyses (e.g., significant differences in professional judgment or differences of opinion on issues that are material to the financial statements or to the final conclusions).***

Records for purposes of this subsection include workpapers and other documents that form the basis of the financial statement engagement; and memoranda, correspondence, communications, and other documents and records that meet both of the criteria stated above.

It is the firm's position that all documents (whether hard copy or electronic) that do not meet **criteria 1 and 2**, above, would not be considered substantive in nature and thus would not have to be retained in accordance with this policy. The firm, however, acknowledges the following exception to this rule:

• All significant information that is inconsistent with the final conclusions, opinions, or analyses (e.g., significant differences in professional judgment or differences of opinion on issues that are material to the financial statements or to the final conclusions) must be considered substantive in nature and appropriately retained in accordance with this policy.

Although this list is not meant to be all-inclusive, the following are examples of those items that generally would not meet the criteria for retention and should be destroyed at the completion of the engagement:

• Superseded drafts of memoranda, financial statements, or regulatory filings

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

• Duplicates of documents

• Copies of client records (unless the client records contain evidence of audit or other procedures applied by the firm)

• Review notes

• To-do lists (that have been completed)

• Documents that contain typographical errors or other minor errors that result from the normal business/learning process or from preliminary views based on incomplete information or data

• Voice mail messages (however, it is the firm's policy that all significant voice mail messages that would record or support the firm's professional services be documented as a memo to file and retained in accordance with the terms of this policy)

***However, if any of the documents listed above DO include information that contains conclusions, opinions, analyses, and/or financial data related to the audit, review, compilation, or preparation, or significant information that is inconsistent with the final conclusions, opinions, or analyses, they will be subject to the retention periods for such information in accordance with the terms of this policy.* [*Note: This paragraph is applicable to states that have conformed to the SEC definition of working papers.*]**

**It is our firm’s policy that any changes in and/or to documentation (including electronic documentation) made by any member(s) of the firm will be required to contain the following:**

• Identification of the person(s) making the change

• Identification of the person(s) approving the change

• Date of the change

• Reason for the change if the reason is not for the assembling of pre-existing documents within a 60-day period after the issuance of the report

The firm makes every effort to comply with all applicable requirements as they relate to the documentation containing sufficient detail regarding the nature, timing, reason for, and extent of the change.

Questions arising in connection with applying the rules set forth in this section should be referred immediately to the partner on the engagement. The Managing Partner must approve any exceptions to this policy.

**Other Services (Includes Tax and Consulting Services)**

<Firm Name> will retain sufficient records (whether hard copy or electronic) to reflect services performed by and substantive information provided to the firm for the engagement for <number (CAMICO recommends no less than five)> years after it completes such services. Records, for the purposes of this subsection, mean final workpapers and any other documents, including correspondence and copies of client records, that are necessary for a reasonable person to understand the services performed by and substantive information provided to <Firm Name> for the engagement but do not include the firm's billing records.

**Administrative Files**

It is the firm's policy that all administrative files (including, but not limited to, billing and collecting activities, accounts payable, loans, leases, fixed assets, and personnel files) will be maintained for no less than the current legal or regulatory requirements for such items or longer if they serve a useful purpose as determined by <Name of Position or Person> and with the approval of the Managing Partner. <Name of Position or Person> will be responsible for maintaining and annually updating a summary of the legal and regulatory requirements for all administrative files and keeping the Managing Partner updated regarding any changes to such requirements.

**Physical Security**

It is company protocol to protect all hard-copy files, electronic files, computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards. As such, the firm has adopted procedures for information maintained in both hardcopy form and electronic form to ensure physical security.

***Hard-Copy Form***

• The firm will store all of its on-site hard-copy client workpaper files in file cabinets. File cabinets are stored in a separate file room and are restricted to those employees authorized to have such access. <Name of Position or Person> has the responsibility for managing the access control of the file room and for reporting any potential breaches in security to the Managing Partner.

• <Name of Position or Person> will have the responsibility for establishing filing procedures to ensure that files can be easily located and retrieved as necessary.

***Electronic Form***

• The firm has established backup procedures for electronic files to minimize the risk that data may be destroyed, modified, or disclosed without authorization. These procedures include, but are not limited to, the following:

– <Name of Position or Person> will be responsible for ensuring that all data files will be backed up <identify time frame (daily, weekly, etc.)> on <identify medium (cloud-based applications, external hard drive, USB flash drives, writable CD/DVD-ROM, etc.)>.

– <Name of Position or Person> will be responsible for ensuring also that all software applications used in creating the work or in archiving or storing the files are retained or available (including all updated or superseded applications) so that the electronic files can continue to be accessed for the retention periods stated in this policy.

– <Name of Position or Person> will be responsible for ensuring that all electronic workpapers are “locked down” at the conclusion of an engagement.

• Access controls have been established to maintain the confidentiality and integrity of data stored on the firm's computer systems. Access shall be restricted to only those actions that are appropriate to each employee's specific job duties. <Name of Position or Person> will have the responsibility for the administration of access controls and will ensure that all additions, deletions, and/or changes are processed appropriately upon written request from the firm administrator, applicable supervisor, and/or partner. Employees will have individual access codes and passwords to the firm's computer network systems. These systems are accessible at all times by the firm, and <Name of Position or Person> will maintain a complete list of access codes and passwords in a secured place. Employees are prohibited from the unauthorized use of the access codes and passwords belonging to other employees. Additional information regarding the firm’s data security policies and procedures can be found in the <specify policy>.

***Refer also to the firm's disaster recovery policy regarding specific recovery procedures if a disaster occurs.***

**Confidentiality**

All of the documents and records relating to clients are the property and proprietary interest of <Firm Name> to the extent it is consistent with applicable laws. All original documents are the property of the client and should be returned to the client upon completion of the engagement. The firm's documents and records relating to clients are confidential and may not be disclosed without the express written permission from the client or unless required by law. All employees of the firm must ensure that privacy will be maintained for client information in accordance with the terms set forth in the firm’s Employee Handbook.

**Destruction of Records**

<Name of Position or Person> has the responsibility for ensuring compliance with this policy for the destruction of records, files, and electronic data. It is the firm's policy that all engagement letters issued on or after the effective date of this policy contain language regarding the firm's applicable record retention period. Refer to Exhibit A for sample language. For engagements prior to the effective date of this policy, or for engagements that did not have engagement letter language addressing the record retention policy, <Name of Position or Person> will make a reasonable attempt to contact the client or former client to inform them of the intent to destroy the records. Notice shall be deemed to be reasonable if given by U.S. mail postage prepaid to <Client Name>’s last known address, whether actually received or not.

The firm will conduct on a <biannual/annual> basis an inventory of all records, files, and electronic data subject to destruction based on the retention periods outlined in Exhibit B, attached. <Name of Position or Person> will review this list with the Managing Partner for approval prior to the actual destruction of such records. Document destruction services are performed by <Name of Company and license numbers> under separate agreement.

***Under no circumstances will any records, files, or electronic data be destroyed, regardless of the retention periods identified in this policy, if there is any pending regulatory investigation, disciplinary action, or legal action, or if the firm has knowledge of the intent by a regulatory agency to launch an inquiry or knowledge of a potential legal claim.***

**Roles and Responsibilities [*Note:* The following is for reference purposes only and will need to be tailored to address the specific roles and responsibilities of the members of your firm.]**

|  |  |
| --- | --- |
|  |  |
| ***Managing Partner*** | • Enforce this record retention and destruction policy  • Annually review and update this policy as needed to ensure compliance with regulatory requirements  • Approve and document exceptions to this policy on an “as needed” basis |
|  |  |
| ***Partners*** | • Enforce this record retention and destruction policy  • Annually review and update this policy as needed to ensure compliance with regulatory requirements |
|  |  |
| ***<Name of Position, e.g.,***  ***Engagement Partner>*** | • Ensure, in accordance with the terms of this policy, that all required documentation (including electronic records) is maintained at the end of the client engagement, and that all original client records are returned to the client  • Confirm with others as necessary that all documentation not required to be retained in accordance with this policy is appropriately destroyed at the end of the client engagement |
|  |  |
| ***Firm Administrator*** | • Maintain and annually update the legal and regulatory requirements for all administrative files, including, but not limited to, personnel documents and payroll records  • Establish and maintain filing procedures and limit the access as appropriate to prevent breaches in security in accordance with the terms of this policy  • Ensure compliance with this policy for the destruction of records, files, and electronic data  • Notify employees of the policy and updates, as appropriate |
|  |  |
| ***Information Systems Manager*** | • Ensure that backup procedures are in place on all electronic files in accordance with the terms of this policy  • Ensure that appropriate access controls are maintained to protect and maintain the confidentiality and integrity of the data stored on the firm's computer systems in accordance with all legal and regulatory requirements |
|  |  |
| ***Managers/Supervisors/Seniors*** | • Ensure that all personnel are aware of and comply with this policy  • Develop and apply appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy |
|  |  |
| ***All Employees and Independent Contractors*** | • Adhere to this policy at all times |

**Employees should notify their immediate supervisor or any member of management upon learning of violations of this policy. Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.**

**Exhibit A**

**Sample Engagement Letter Language Re: Record Retention** **Exhibit A Sample Engagement Letter Language Re: Record Retention**

It is our policy to keep records related to this engagement for <number> years. However, <Firm Name> does not keep any original client records, so we will return those to you at the completion of the services rendered under this engagement. When records are returned to you, it is your responsibility to retain and protect your records for possible future use, including potential examination by any government or regulatory agencies.

**By your signature below, you acknowledge and agree that upon the expiration of the <number>-year period <Firm Name> shall be free to destroy our records related to this engagement**.

**Exhibit B**

**Record Retention Periods: Engagement Files**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | ***Retention Period[[1]](#footnote-1)*** | |
|  | ***Current Client*** | ***Former Client*** |
| Billing Files | 7 years | 7 years |
| Correspondence Files | 7 years | 7 years |
| Audit/Review/Compilation Statements and Reports | Permanently | 7 years |
| Tax Returns | Permanently | 5 years |
| Special Reports | Permanently | 5 years |
|  |  |  |
| **Workpaper Files:** | | |
| • Audit/Review/Compilation Workpapers | 7 years | 7 years |
| • Tax Return Workpapers | 5 years | 5 years |
| • All Other Services | 5 years | 5 years |
| • Permanent/Carryforward Files (Audit/Review/Compilation Services) | Permanently | 7 years |
| • Permanent/Carryforward Files (Other Services) | Permanently | 5 years |

**Other Files:**

• <List>

1. The retention periods noted are for illustration purposes only. Firms need to ensure that they are complying with applicable state, regulatory, and professional requirements. From a risk management perspective, a firm may want to consider retaining client records (regardless of service) for the same length of time as long as the period of time satisfies the most stringent requirement to ease the compliance burden. [↑](#footnote-ref-1)