Disaster Recovery Policy

1. Overview

The purpose of this policy is to provide standards of practice to limit business interruption given a human induced or natural disaster.

2. Data Storage and Data Privacy

All data is stored on the CompTeam Google Drive and backed up to an encrypted physical drive each Friday. No client employee level or confidential data may be stored on individual computers. Confidential client information must be stored on their respective internal servers or cloud storage approved by the client company. CompTeam data may be found on 1) the CompTeam Google Drive, 2) the Google Takeout System, and an encrypted, secured physical back-up locked in a fire proof safe.

As the Internet is a global environment, collecting and processing confidential client information may involve the transmission of this data internationally, including into and/or outside of the United States. Therefore, all clients acknowledge and agree to its confidential client information being processed in this way. Confidential client information collected or received by CompTeam from clients or third parties may be stored and processed in the United States or any other country where we or our service providers maintain facilities. The servers and databases in which information is stored may be located outside the country from which the client resides, and in a country that does not have the same privacy laws as its country of residence. The confidential client information you provide us may be transmitted abroad, but we will collect, process and use confidential client information only in accordance with CompTeam's policies.

3. Computer Systems

Computers, mobile phones and tablets are to be used as a terminal accessing cloud services. Software programs such as Adobe, MS Office, etc. should be cloud based to the greatest extent as possible.

4. Internet Connectivity

The principle method of connectivity is a secured wire internet connection. A secured cellular network and MiFi connection are used remotely. Open and unsecured internet connections are to be avoided.

5. Equipment Replacement Plan

Desktops, laptops, tablets and phones are to be replaced as needed. Physical back-up drive is checked quarterly via diagnostic tool and replaced as needed. No single piece of equipment is necessary for business continuity.

Security Incident Management Policy

1. Overview

The purpose of Incident Management within CompTeam is to properly handle security incidents and execute upon security incident management.

2. Preparation

All employees/contractors that maintain or handle Confidential Information – either Customer Information or Internal CompTeam Confidential Information, have implemented the following processes:

- All employees/contractors have security awareness training
- All employees/contractors are to immediately notify Sam Reeve of any actual or suspected incident and/or security breach.

Employees, including all full time, temporary, or contract are included in policies that enforce:

- Using unique combination passwords. (see Access Control and Password Policy)
- Quarterly password changes.
- Instructed to never share passwords with others.
- Encrypting information when it is transmitted electronically.
- Referring calls or other requests for personal information to Sam Reeve.

Detection and analysis mechanisms include:

- Automated detection and eradication tools
- Automated notification of logins from other systems

3. Containment, Lock Down and Communication

Once a security breach has been validated, staff members will immediately power down the system and remove from the internet/network. All suspected security incidents will be immediately reported to Sam Reeve for further analysis. Sam Reeve will be responsible for all internal and external communication of the incident.

4. Eradication and Recovery

Sam Reeve is responsible for coordinating the containment of the incident using whatever means is necessary to limit and contain customer impact. Once a security incident has been contained, eradication is necessary to eliminate components of the incident, such as removing malicious code or disabling compromised user accounts. Recovery involves restoring information as closely as possible back to the point just before the incident occurred. Adjusting monitoring and reviewed/adjusted security measures.

Access Control and Password Policy

1. Overview

Computer accounts are used to manage security privileges and grant access to CompTeam information systems and applications. The process of creating, controlling, managing, and monitoring computer accounts is critical to a comprehensive security program.

2. Purpose

Identification and authentication access controls play an important role in helping to protect information systems and the data contained within them. The purpose of this policy is to define requirements, procedures, and protocols for managing access control and passwords within CompTeam.

3. Scope

This policy applies to all CompTeam staff, users, and contractors that use, create, deploy, or support application and system software. This policy applies to all computer assets and software regardless of ownership.

4. Policy

A. GENERAL

The Consultant/Contractor shall ensure that policies and procedures are followed:

- Manage the process of creating, changing, and safeguarding passwords/phrases
- Prevent staff from sharing passwords/phrases with others
- Advise staff to commit their passwords/phrases to memory and not allow them to be written down (use a password vault)
- Govern password/phrase change frequency
- Dictate when passwords/phrases must be supplemented with additional access controls such as “smart” card, tokens, or other supplemental two and/or three factor authentication verification procedures

This Policy applies to all CompTeam related authentication activities including but not limited to the following types of computer hardware, application, and device based accounts:

- Systems administrative
- Role-based administrative
- End-user accounts
- Network infrastructure devices (e.g. firewalls, routers, wireless access points, etc.)
- Third party service providers
- Web applications
- Screen savers
- Mobile devices

B. NEW USER ACCOUNTS

When creating and granting access for a new end user account:

- System administrators shall establish a unique ID and unique password/phrase separate from their regular user account
- End user passwords will be conveyed to staff and customers in a secure manner

- End users will be required to change their initial password/phrase to something that adheres to policy and is known only to that user

C. SELECTING PASSWORDS/PHRASES

All users shall select passwords/phrases that meet requirements for being strong and complex. Staff shall be required to choose passwords/phrases that meet the following requirements:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Include both numbers (0-9) and special characters (e.g. @, #, $, *)
- Have a minimum of at least 8 characters (preferably 10 characters long or more) and are phrase based
- Where possible, use different passwords/phrases for general office activities (e.g. e-mail, file access) vs. systems that store sensitive or confidential data

Password attributes shall be enforced through a password group policy applied to the CompTeam workforce. Staff shall not choose passwords/phrases that:

- Include common words found in a dictionary
- Are the same as passwords/phrases used on personal accounts (e.g. email, online banking, or social media)
- Contain personal information such as a spouse or pet's name, Social Security Number, driver's license number, street address, phone number, etc.
- Contain sequences or repeated characters (1234, 3333, etc.)

Staff with special system privileges, assigned by a transaction, program, process, or group membership, should select a unique password/phrase from other accounts held by that individual.

Generic user accounts shall not be authorized for use by staff on any CompTeam based computer applications or hardware.

D. PASSWORD/PHRASE GUIDELINES

Staff shall follow this CompTeam security policy and guideline to ensure passwords/phrases are not compromised. Security training shall ensure staff are educated and reminded of:

- Security related risks of lax password procedures
- CompTeam requirements in selecting and protecting passwords/phrases
- Not selecting the "Remember Me" or "Remember Password" feature in web applications and browsers
- Cautions when using social media so a password/phrase combination is not compromised

Additionally, passwords and passphrases must not be:

- Revealed or shared with any other individual
- Stored, written down, or transmitted in clear (unencrypted) text
- Inserted into unencrypted email messages or other forms of electronic communications

Should a staff member believe their password/phrase has been compromised or made available to others, they must immediately reset/change their password and notify Sam Reeve at CompTeam.

E. PASSWORD/PHRASE CHANGES

Passwords/phrases shall be changed on a regular basis according to the following schedule:

- Administrative passwords/phrases must be changed at least every 60 days.
- User passwords/phrases must be changed at least every 90 days.
- Staff shall not repeat any of their prior five passwords/phrases.

F. SOFTWARE APPLICATIONS

Application developers must ensure programs contain the following security precautions:

- Applications must require each end user to have their own unique user ID (e.g. generic, shared, service, or group based accounts are disallowed). It is acceptable to use security groups for access control lists to certain features and functions of an application
- Passwords/phrases and sensitive information shall be protected using at-rest and in-transit encryption
- Passwords/phrases and sensitive information shall not be transmitted or stored in clear text
- Application timeout standards shall be enforced and require a user to re-enter a password/phrase after a period of inactivity to regain access to their application

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the CompTeam internal application development and release methodology. Examples of control procedures shall be demonstrated through regular and repeatable administrative processes as follows:

- Documented and demonstrable access control group policy around strong password and history requirements.
- Annual audits of directory accounts for ‘dead’ account scavenging process.
- Appropriate logging, alerting and reporting of security events within applications and server based access.

6. Enforcement

Staff members are responsible for maintaining the confidentiality and security of their username and password in addition to complying with this Policy. Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all CompTeam staff and contractors using CompTeam information resources.

Data Backup Policy

1. Overview

The purpose of this policy is to provide consistent rules for backup management to ensure backups are available when needed.

2. Data to be Backed Up

All data stored on the CompTeam Google Drive servers, email servers, web servers, will be backed up. It is the user's responsibility to ensure any data of importance is maintained on the CompTeam Google Drive server.

3. Back Up Frequency, Process and Duration

The CompTeam Google Drive servers, email servers, web servers, are backed up each Friday using the Google Takeout system. Each backup zip file should be no large than 2GB and stored on secured backup drive. A weekly backup is retained for a one month period.

4. Back Up Storage

When stored onsite, backup media must be stored in a locked fireproof safe in an access-controlled area. When moved offsite, a hardened facility (i.e., commercial backup service) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media and that all Service Level Agreements for clients are met.

Data Privacy Policy

1. Overview

CompTeam is committed to protecting the privacy and confidentiality of Personal Information about its employees, contractors, customers, business partners and other identifiable individuals. CompTeam's policies, guidelines and actions support this commitment to protecting Personal Information. Each employee/contractor bears a personal responsibility for complying with this Policy in the fulfillment of their responsibilities at CompTeam.

2. Scope

This Policy sets the minimum standard and shall guide all CompTeam employees/contractors and Agents even if local law is less restrictive. Supplemental policies and practices will be developed as needed to meet the local legal or departmental requirements. Supplemental policies and practices may provide for more strict or specific privacy and protection standards than are set forth in this Policy.

CompTeam does not knowingly or intentionally collect information from children under 13, pursuant to the Children's Online Privacy Protection Act ("COPPA"). All information provided to us will be treated as if it was provided by an adult. We will use commercially reasonable efforts to delete information associated with a child under 13 as soon as practicable once discovered.

3. Policy Details

CompTeam respects the privacy of its employees/contractors and third parties such as customers, business partners, vendors, service providers, suppliers, former employees/contactors and candidates for employment and recognizes the need for appropriate protection and management of Personal Information. CompTeam is guided by the following principles in Processing Personal Information:

- Notice
    - When collecting Personal Information directly from individuals, CompTeam strives to provide clear and appropriate notice about the:
        - Purposes for which it collects and uses their Personal Information,
        - Types of non-Agent third parties to which CompTeam may disclose that information, and
        - Choices and means, if any, CompTeam offers individuals for limiting the use and disclosure of their Personal Information.

- Choice
    - Generally, CompTeam offers individuals a choice regarding how we Process Personal Information, including the opportunity to choose to opt-out of further Processing or, in certain circumstances, to opt-in. However, explicit consent from individuals is not required when Processing Personal Information for:
        - Purposes consistent with the purpose for which it was originally collected or subsequently authorized by the individual,
        - Purposes necessary to carry out a transaction relationship,
        - Purposes necessary to inspect and resolve a suspected violation of customer agreements;
        - Disclosure to an Agent; or
        -
        - Purposes necessary to comply with legal requirements, including but not limited to:
            - Responding to requests from public/government authority to meet national security or law enforcement requirements;

- Comply with a judicial proceeding, subpoena, court order, or legal process; or
- To otherwise protect our rights, or act under emergency circumstances to protect the personal safety of CompTeam.

- Accountability for onward transfer
    - In regard to the transfer of Personal Information to either an Agent or Controller, CompTeam strives to take reasonable and appropriate steps to:
        - Transfer such Personal Information only for specified purposes and limit the Agent or Controller's use of that information for those specified purposes,
        - Obligate the Agent or Controller to provide at least the same level of privacy protection as is required by this Policy,
        - Help ensure that the Agent or Controller effectively Processes the Personal Information in a manner consistent with its obligations under this Policy,
        - Require the Agent or Controller to notify CompTeam if the Agent or Controller determines it can no longer meet its obligation to provide the same level of protection as is required by this Policy, and
        - Upon notice from the Agent or Controller, take further steps to help stop and remediate any unauthorized Processing.

- Security
    - CompTeam takes reasonable and appropriate measures to protect Personal Information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the Processing and the nature of the Personal Information.

- Data integrity and purpose limitation
    - CompTeam will only Process Personal Information in a way that is compatible with the purpose for which it has been collected or subsequently authorized by the individual or company. CompTeam shall take steps to help ensure that Personal Information is accurate, reliable, current and relevant to its intended use.

- Access
    - CompTeam provides individuals with reasonable access to their Personal Information for purposes of correcting, amending or deleting that information where it is inaccurate or has been Processed in violation of the CompTeam data privacy principles.

- Recourse, Enforcement and Liability
    - Violation of this Policy by an employee or contractor of CompTeam will result in appropriate discipline up to and including termination. Violation by an Agent, Controller or other third party of this Policy or CompTeam's privacy requirements will result in the exercise of appropriate legal remedies available at law or in equity including termination for material breach of contract.

4. Purpose of Collecting and Use of Personal Information

CompTeam may from time to time Process certain Personal Information from or about employees/contractors and third parties such as customers, business partners, vendors, service providers, suppliers, former employees and candidates for employment, including information recorded on various media as well as electronic data.

CompTeam will use that Personal Information to provide customers, business partners, vendors, service partners and suppliers with information and services and to help CompTeam personnel better understand the needs and interests of these customers, business partners, vendors, service partners and suppliers.

Specifically, CompTeam uses information to help complete a transaction or order, to facilitate communication, to market and sell products and services, to deliver products/services, to bill for purchased products/services, and to provide ongoing service and support. Occasionally CompTeam personnel may use Personal Information to contact customers, business partners, vendors, service partners and suppliers to complete surveys that are used for marketing and quality assurance purposes.

CompTeam may also share Personal Information with its business partners, vendors, service providers and suppliers to the extent needed to support the customers' business needs. Suppliers are required to keep confidential Personal Information received from CompTeam and shall not use it for any purpose other than as originally intended or subsequently authorized or permitted.

CompTeam also collects client Human Resources Data in connection with consulting services for our clients. These programs and functions may include compensation and benefit programs, employee level pay data, employee development planning and review, performance appraisals, training, employee profiles, internal employee directories, Human Resource record keeping, and other employment related information. Human Resources Data may be shared with third party vendors and service providers with the client's consent, for the purpose of enabling the vendor or service provider to provide service and/or support to CompTeam in connection with the consulting agreement with the Client. CompTeam requires third parties receiving Personal Information to apply the same level of privacy protection as contained in this Policy and as required by applicable law.

Separate from client engagements, CompTeam also collects and uses Personal Information to consider candidates for employment or contract opportunities within CompTeam. CompTeam does not sell or trade Personal Information to third parties.

5. Data Administration

Responsibility for compliance with this Policy rests with the heads of the individual functions and any individual employees/contractors collecting, using or otherwise Processing Personal Information. Sam Reeve is responsible for implementing further standards, guidelines and procedures that uphold this Policy, and for assigning day-to-day responsibilities for privacy protection to specific personnel for enforcement and monitoring.

- Interpretation
    - In the event of any conflict between this Policy and any supplemental data privacy policy, this Policy will supersede the supplemental data privacy policy to the extent that the supplemental data privacy policy is less restrictive. Local data privacy policies may provide for stricter data privacy and protection standards than are set forth in this Policy. In the event local data privacy law provides for stricter data privacy and protection than this Policy, the local data privacy law will supersede this Policy in that jurisdiction to the extent necessary to comply with stricter local law.
- Data Retention
    - All CompTeam employees/contractors who process data for CompTeam or it's clients must not keep data for longer than is necessary to complete the work. It is a matter for reasonable judgement and common sense as to how long personal data should be retained. In many instances the retention of personal data will be necessary and thus justified for a significant period of time. In the case of a completed client project, a single copy of the work may be archived by Sam Reeve for legal reasons or to support the future needs of the client.

6. Merger, Sale or Bankruptcy

Personal Information may be disclosed or distributed to another party with which CompTeam enters, or may enter, into a corporation transaction. If CompTeam is acquired in a merger, acquisition, or sale of all or substantially all its assets, it will take the necessary steps to provide notice to customers and

employees in addition to any change in the uses of their Personal Information, as well as any choices you may have regarding their Personal Information. The disclosure of Personal Information to another party as set forth herein may involve the transfer of such Personal Information outside the state, province, country or other jurisdiction in which CompTeam stores or otherwise Processes Personal Information, subject to CompTeam taking steps to provide that any such transfer is made only in compliance with applicable laws. In the unlikely event of a bankruptcy, insolvency or liquidation, the database containing Personal Information may be treated as an asset of CompTeam and may be subject to transfer to a third party.

7. Definitions

“Agent” means any third party that collects and/or uses Personal Information provided by CompTeam to perform tasks on behalf of and under the instructions of CompTeam.

“CompTeam” is CompTeam, LLC

“Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

“Human Resource Data” means Personal information concerning CompTeam employees/contractors, prospective employees/contractors or a clients workforce information needed for defined project work. An “Identified” or “Identifiable” individual is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the person’s physical, physiological, mental, economic, cultural or social identity.

“Personal Information” is information or data about an “Identified” or “Identifiable” (see definition above) individual. It does not include information that is anonymous, aggregated or in circumstances where the individual is not readily identifiable.

“Policy” means this Data Privacy Policy.

“Processing” or “Process” means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Retention Policy

1. Overview

The purpose of this Policy is to ensure that necessary records and documents of are adequately protected and maintained and to ensure that records that are no longer needed by CompTeam or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees/contractors of CompTeam in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

2. Overview

This Policy represents CompTeam's policy regarding the retention and disposal of records and the retention and disposal of electronic documents.

3. Administration

Attached as Appendix A is a Record Retention Schedule that is approved as the initial maintenance, retention and disposal schedule for physical records of CompTeam and the retention and disposal of electronic documents. Sam Reeve (the "Administrator") is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. The Administrator is also authorized to: make modifications to the Record Retention Schedule from time to time to ensure that it is in compliance with local, state and federal laws and

includes the appropriate document and record categories for CompTeam; monitor local, state and federal laws affecting record retention; annually review the record retention and disposal program; and monitor compliance with this Policy.

4. Suspension of Record Disposal In Event of Litigation or Claims

In the event CompTeam is served with any subpoena or request for documents or any employee/contractor becomes aware of a governmental investigation or audit concerning CompTeam or the commencement of any litigation against or concerning CompTeam, such employee shall inform the Administrator and any further disposal of documents shall be suspended until shall time as the Administrator, with the advice of counsel, determines otherwise. The Administrator shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.

5. Applicability

This Policy applies to all physical records generated in the course of CompTeam's operation, including both original documents and reproductions. It also applies to the electronic documents described above.

This Policy was approved by Sam Reeve of CompTeam on January, 1st 2019.

APPENDIX A - RECORD RETENTION SCHEDULE

The Record Retention Schedule is organized as follows:

SECTION TOPIC
- A. Accounting and Finance
- B. Contracts
- C. Business Records
- D. Correspondence and Internal Memoranda
- E. Electronic Documents
- F. Insurance Records
- G. Legal Files and Papers
- H. Miscellaneous
- I. Payroll Documents and Personnel Records
- J. Tax Records

A. ACCOUNTING AND FINANCE

Record Type	Retention Period
Accounts Payable ledgers and schedules	5 years
Accounts Receivable ledgers and schedules	Collection plus 5 years
Annual Audit Reports and Financial Statements	Permanent
Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual Plans and Budgets	2 years
Bank Statements and Canceled Checks	7 years
Employee Expense Reports	6 years
General Ledgers	Permanent
Interim Financial Statements	6 years
Notes Receivable ledgers and schedules	Collection plus 5 years
Investment Records	7 years after sale of investment
Credit card records (documents showing customer credit card number)	2 years

<u>Credit card record retention and destruction</u>
A credit card may be used to pay for consulting products and services:
- Project work
- Retained service agreement

All records showing customer credit card number must be held in a secure location when not in immediate use by staff.

If it is determined that information on a document, which contains credit card information, is necessary for retention beyond 2 years, then the credit card number will be cut out of the document.

B. CONTRACTS

Record Type	Retention Period
Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documentation)	6 years after expiration or termination

C. BUSINESS RECORDS

Record Type	Retention Period
Business Records (minute books, signed minutes of the Board and all committees, corporate seals,	Permanent

articles of incorporation, bylaws, annual corporate reports)	
Licenses and Permits	Permanent

D. CORRESPONDENCE AND INTERNAL MEMORANDA

General Principle: Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded within one years. Some examples include:

   - Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
   - Form letters that require no follow-up.
   - Letters of general inquiry and replies that complete a cycle of correspondence.
   - Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change).
   - Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
   - Chronological correspondence files.

Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

E. ELECTRONIC DOCUMENTS

1. Electronic Mail: Not all email needs to be retained, depending on the subject matter.

- All e-mail—from internal or external sources—is to be deleted after 12 months.
- Staff will strive to keep all but an insignificant minority of their e-mail related to business issues.
- CompTeam will archive e-mail for six months after the staff has deleted it, after which time the e-mail will be permanently deleted.
- All CompTeam business-related email should be downloaded to a user directory on the server.
- Staff will not store or transfer CompTeam-related e-mail on non-work-related computers except as necessary or appropriate for CompTeam purposes.
- Staff will take care not to send confidential/proprietary CompTeam information to outside sources.
- Any e-mail staff deems vital to the performance of their job should be copied to the CompTeam Google Drive.

2. Electronic Documents: including Microsoft Office Suite and PDF files. Retention also depends on the subject matter.

- PDF documents – The length of time that a PDF file should be retained should be based upon the content of the file and the category under the various sections of this policy. If the subject matter of the PDF does not otherwise fall into a category enumerated by this policy, it should

be retained for 6 years. PDF files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace.

- Text/formatted files - Staff will conduct annual reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those they consider unnecessary or outdated. If the text file is determined to be unnecessary or outdated, it will be deleted from the network and the staff's desktop/laptop. Text/formatted files the staff deems vital to the performance of their job should be printed and stored in the staff's workspace.

F. INSURANCE RECORDS

Record Type	Retention Period
Annual Loss Summaries	10 years
Audits and Adjustments	3 years after final adjustment Certificates Issued to CompTeam
Claims Files (including correspondence, medical records, injury documentation, etc.)	Permanent
Group Insurance Plans - Active Employees	Until Plan is amended or terminated
Group Insurance Plans – Retirees	Permanent or until 6 years after death of last eligible participant
Inspections	3 years
Insurance Policies (including expired policies)	Permanent
Journal Entry Support Data	7 years
Loss Runs	10 years
Releases and Settlements	25 years

G. LEGAL FILES AND PAPERS

Record Type	Retention Period
Legal Memoranda and Opinions (including all subject matter files)	Case by case basis
Litigation Files	Case by case basis
Court Orders	Permanent
Requests for Departure from Records Retention Plan	10 years

H. MISCELLANEOUS

Record Type	Retention Period
Consultant's Reports	2 years
Material of Historical Value (including pictures, publications)	Permanent
Policy and Procedures Manuals – Original	Current version with revision history
Annual Reports	Permanent

I. PAYROLL DOCUMENTS

Record Type	Retention Period
Employee Deduction Authorizations	6 years after termination
Payroll Deductions	6 years after termination
W-2 and W-4 Forms	4 years after later of due date/payment of tax
Garnishments, Assignments, Attachments	6 years after termination
Labor Distribution Cost Records	6 years after termination
Payroll Registers (gross and net)	6 years
Time Cards/Sheets	3 years
Unclaimed Wage Records	10 years

J. PAYROLL DOCUMENTS AND PERSONNEL RECORDS

Record Type	Retention Period

Commissions/Bonuses/Incentives/Awards	6 years
EEO- I /EEO-2 - Employer Information Reports	Keep most recent report on file
Employee Earnings Records	Permanent
Employee Handbooks	1 copy kept permanently
Employee Medical Records	Separation + 30 years
Employee Personnel Records (including individual attendance records, application forms, job or status change records, performance evaluations, termination papers, withholding information, garnishments, test results, training and qualification records)	3 years after separation
Employment Contracts – Individual	6 years after separation
Employment Records - Correspondence with Employment Agencies and Advertisements for Job Openings	1 year from date of hiring decision
Employment Records - All Non-Hired Applicants (including all applications and resumes - whether solicited or unsolicited, results of post-offer, pre-employment physicals, results of background investigations, if any, related correspondence)	5 years
Job Descriptions	2 years after superseded
Personnel Count Records	3 years
Forms I-9	3 years after hiring, or 1 year after separation if later

K. TAX RECORDS

Record Type	Retention Period
IRS Rulings	Permanent
Excise, Payroll Tax Records	7 years
Tax Bills, Receipts, Statements	Permanent
Tax Returns	Permanent
Tax Workpaper Packages - Originals	Permanent
Sales/Use Tax Records	Permanent
Annual Information Returns - Federal and State	Permanent
IRS or other Government Audit Records	Permanent