Document Retention Policy

I. Purpose

The document retention policy exists to reduce risks, eliminate waste, and abide by relevant laws by specifying procedures pertaining to the retention, storage and deletion of physical and digital records.

II. Scope

This policy affects all Nested Knowledge employees, contractors, consultants, and business partners.

Digital records include contracts, operating agreements, tax returns, emails, chats, voice messages, invoices, meeting notes, presentations, scanned documents submitted by employees or external sources, and social media posts.

Physical records may include contracts and completed tax forms.

III. Policy

(A) Document Retention - Internal Company Documents

Tax Returns

Nested Knowledge will keep tax-related records for at least **eight years,** or until acquired.

Payroll

Nested Knowledge will keep payroll records for **three years**, or until acquired.

Retirement Plans

Nested Knowledge has implemented a 401(k) plan. All documentation will be maintained in accordance with Employee Retirement and Income Security Act (ERISA).

Health Insurance

Records related to health insurance are subject to retention rules specified by the Health Insurance Portability and Accountability Act (HIPAA).

Employee Records

Records to employees, such as benefits, time tracking, performance evaluations, or training documents should be stored in an accessible, secure digital location. Records should be kept for **three years** following the employees termination (or until company is acquired).

- Nested Knowledge managers should store performance evaluations in the Google Drive, which is accessible only to Nested Knowledge managers and the executive team.

Other Business Records

According the Uniform Preservation of Business Records Act, documents not covered under any particular statute can be destroyed after **three years.** Nested Knowledge employees will be encourage to destroy digital documents after three years to preserve storage spaces.

Suspension for Litigation

In the event of active or imminent litigation, the above policy will be suspended.

(B) Data Retention by Data Class

Retention of personal data shall be alligned with our Data Classification scheme.

Data Class	Description	Retention Procedure	Legal Regulations
Public Data	Data that may be disclosed to anyone, regardless of their affiliation with Nested Knowledge.	Public data will be reviewed at least annually for relevance and accuracy and may be deleted at will.	No specific retention period is mandated.
Internal Company Data	Potentially sensitive information not intended for public sharing.	Internal data shall be retained according the guidance in Part A of this policy.	Internal documents may be subject to requirements from ERISA, HIPAA, and the Internal Revenue Code.
Confidential Data	Information that, if made available to unauthorized parties, may adversely affect individuals, partner organizations, or Nested Knowledge.	Confidential data shall be retained for a period of **3 years,** or as required by applicable contractual and regulatory requirements, whichever is longer.	

Restricted Use Data: Emails, Filesystems, and Support Applications	Information that Nested Knowledge has a contractual, legal, or regulatory obligation to safeguard stringently. This includes Personally Identifiable Information and Unencrypted data used to authenticate or authorize individuals	Restricted use data shall be retained for a period of **3 years,** or as required by applicable contractual and regulatory requirements, whichever is longer.	
Restricted Use Data: Customer Personal Data	This includes personally identifiable information as well as project data stored in the Nested Knowledge production databases. We collect name, email address, and (optionally) organization name from users.	Personal data are stored in our production database, within a VPC. All communication with the database is encrypted and behind authorization. **Upon user action through the application initiating deletion of the user's account, all user data is hard deleted.** Database backups, which include customer personal data (names and email addresses), are retained for 60 days.	GDPR data retention rules require personal data that is collected or processed to be kept only for as long as data are required to achieve the purpose for which the information was collected, with the exception of data for scientific research.

Communication and Compliance

This policy will be updated on an annual basis and leadership will regularly oversee this policy to make sure employees are consistently upholding the policy's rules.

Revision History

Any exceptions to the regulations above must be approved by the CEO, CTO, or COO.

Author	Date of Revision/Review	Comments
P. Olaniran	10/31/2022	Draft sent for approval.
K. Kallmes	10/31/2022	Draft approved.
K. Cowie	06/15/2023	Updated
K. Kallmes	6/15/2023	Approved.

Return to Policies