Data Retention Policy

Sweet Adelines is hereinafter referred to as "the organization."

1.0 Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the organization's guidelines on retention are consistently applied throughout the organization.

2.0 Purpose

The purpose of this policy is to specify the organization's guidelines for retaining different types of data.

3.0 Scope

The scope of this policy covers all organization data stored on organization-owned, organization-leased and otherwise organization-provided systems and media, regardless of location.

4.0 Policy

4.1 Reasons for Data Retention

The organization does not wish to simply adopt a "save everything" approach. That is not practical or cost-effective and would place an excessive burden on the organization and IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect the organization's interests, preserve evidence, generally conform to good business practices, and carry out daily business functions. Some reasons for data retention include, but are not limited to:

- Membership Status
- Member Communications
- Human Resources
- Financial Reporting
- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation
- Donor processing

4.2 Data Duplication

As data storage increases in size and decreases in cost, organizations often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the organization's data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

4.3 Retention Requirements

This section sets guidelines for retaining the different types of organization data.

Personal Member Data: In accordance with Section 16 of the Privacy Policy, we only keep your personal information for as long as is reasonably necessary to fulfil the relevant purposes, or longer if required by law.

Donor Data: In accordance with Section 16 of the Privacy Policy, we only keep your personal information for as long as is reasonably necessary to fulfil the relevant purposes, or longer if required by law. Please refer to the Data Retention and Destruction Policy at the end of this document for minimum time requirements for various documents

Employee Data: Please refer to the Data Retention and Destruction Policy at the end of this document for minimum time requirements for various documents. Please refer to the Retention of Terminated Employee Records at the end of this document for minimum time requirements for various documents.

4.4 Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

4.5 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the organization will use data efficiently thereby making data management and data retrieval more cost effective. Exactly when certain data should be destroyed is covered in the charts attached.

When the retention timeframe expires, the organization must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to the organization so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the organization's management team.

The organization specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself is particularly forbidden, or destroying data in an attempt to cover up a violation of law or organization policy.

4.6 Applicability of Other Policies

This document is part of the organization's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of organization property (physical or intellectual) are suspected, the organization may report such activities to the applicable authorities.

6.0 Definitions

Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption: The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Encryption Key: An alphanumeric series of characters that enables data to be encrypted and decrypted.

Retention of Terminated Employee Records

Record Types	Retention Periods
Health & Benefits Records	
Health & Benefits Beneficiary Forms	Termination + 3 yrs.
Medical, Dental/Vision Plan Elections	Termination + 3 yrs.
Drug Test Results	Termination + 3 yrs.
Education Assistance Program Records	Termination + 3 yrs.
FMLA Leave Reports	Termination + 3 yrs.
USERRA Leave Records	Permanent
Toxic & Bloodborne Pathogens Records	Termination + 30 yrs.
Job Related Injuries & illnesses Records	Termination + 5 yrs.
Reasonable Accommodation Records	Termination + 3 yrs.
Pre-Employment/Employment Documents*	
Job Description	Termination + 3 yrs.
Position Requisition	Termination + 3 yrs.
Recruitment Notice/Job Ads	Termination + 3 yrs.
Employment Application/Resume	Termination + 3 yrs.
Interview Evaluation	Termination + 3 yrs.
Assessment Results	Termination + 3 yrs.
Background Check Information	Termination + 3 yrs.
References/Verifications	Termination + 3 yrs.
New-Hire Action Form	Termination + 3 yrs.
Offer Letter	Termination + 3 yrs.
Form I-9	Termination + 3 yrs.
EEO Data Form	Termination + 3 yrs.
Employee Policy Acknowledgements	Termination + 3 yrs.
Conflict of Interest Statement	Termination + 3 yrs.
Intellectual Property Ownership/Nondisclosure	Termination + 5 yrs.
Employee Development Records	Termination + 3 yrs.
Position/Pay History Records	Termination + 3 yrs.
Employee Performance Reviews	Termination + 3 yrs.
International Assignment Documents	Termination + 3 yrs.
Relocation Agreement	Termination + 3 yrs.
Resignation Letter	Termination + 3 yrs.
Termination Action Form	Termination + 3 yrs.
COBRA Election Notice	Termination + 3 yrs.
Separation Agreement	Termination + 5 yrs.
Exit Interview Form	Termination + 3 yrs.
Unemployment Claim Records	Termination + 4 yrs.

SWEET ADELINES INTERNATIONAL

Retention of Terminated Employee Records (continued)

Record Types	Retention Periods
Retirement	
401(k) Allocation Records	Termination + 4 yrs.
401(k) Loan Payment Forms	Termination + 3 yrs.
Pension Eligibility Records	Termination + 50 yrs.
Request for Calculation	Termination + 4 yrs.
Retirement Beneficiary Form	Termination + 50 yrs.
Payroll/Tax	
Paychecks/stubs, W-2s, W-4s	4 yrs.
Earnings Register	4 yrs.
Employee Withholding	4 yrs.
Expense Reports	3 yrs.
Federal & State Payroll Tax Forms	4 yrs.
Federal Forms 1099	4 yrs.
Time Sheets/Cards	4 yrs.
Other Payroll Records	
Computer Loan Agreement	Termination + 5 yrs.
Direct Deposit Records	Termination + 4 yrs.
Garnishment Records	Termination + 4 yrs.
Final Payroll Deduction Checklist	Termination + 4 yrs.
HR Policies & Reports	
EEO-1 Reports	Permanent
HR Policies	While current + 3yrs.
State New-Hire Reports	3 yrs.
Affirmative Action Plans/Records	5 yrs.
Form 5500	6 yrs.
OSHA 300/300A	Posting date + 5 yrs.
VETS-4212 Reports	5 yrs.
[Company Name] Ethics Hotline Reports*	3 yrs.

*Note: If an applicant is ultimately not hired, the above records should be retained for three (3) years after the no-hire decision is made.

SWEET ADELINES INTERNATIONAL

Data Retention and Destruction Policy

Type of Document	Minimum Requirement
Accounts payable ledgers and schedules	7 years
Audit Reports	Permanently
Bank reconciliations	2 years
Bank statements	3 years
Checks (for important payments and purchases)	Permanently
Contracts, mortgages, notes, and leases (expired)	7 years
Contracts (still in effect)	Contract period
Correspondence (general)	2 years
Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2 years
Deeds, Mortgages, and bills of sale	Permanently
Depreciation schedules	Permanently
Duplicate deposit slips	2 years
Employment applications	3 years
Expense analyses/expense distribution schedules	7 years
Year-end financial statements	Permanently
Insurance records, current accident reports, claims, policies, and so on (active and expired)	Permanently
Internal audit reports	3 years
Inventory records for products, materials, and supplies	3 years
Invoices (to customers, from vendors)	7 years
Minute books, bylaws, and charter	Permanently
Patents and related papers	Permanently
payroll records and summaries	7 years
Personnel files (terminated employees)	7 years
Retirement and pension records	Permanently
Tax returns and worksheets	Permanently
Timesheets	7 years
Trademark registrations and copyrights	Permanently
Withholding tax statements	7 years