Family Law Software
A CENTERBASE COMPANY

Data Archive Policy

This document defines the organization's policy for the systematic archival of data, ensuring compliance with legal and regulatory retention requirements while managing storage costs and maintaining data integrity.

1. Scope and Applicability

This policy applies to all structured and unstructured data that has reached the end of its active operational life but must be retained for legal, regulatory, or historical purposes. This includes data moved from primary production systems to secondary, long-term, and low-cost storage.

2. Policy Governance

2.1. Policy Review

This Data Archive Policy document will be formally **reviewed and approved by management at least on an annual basis** (or upon changes in regulatory requirements or business needs) to ensure continued relevance and compliance.

2.2. Archive Definition

Archived data is defined as data that:

1. Is no longer required for day-to-day business operations.
2. Must be kept for a specific retention period.
3. Is stored on media optimized for low-cost, long-term retention (e.g., tape, cold cloud storage).
4. Is infrequently accessed, and access may involve a delay.

3. Data Retention and Archival Requirements

The **data archive policy specifies retention periods** for maintaining data based on legal, regulatory, and business requirements. Once the retention period has expired, the data must be securely and permanently disposed of.

Data Category	**Regulatory Requirement / Business Need**	**Retention Period**	**Post-Retention Action**
Financial Records	Tax/Audit Compliance	7 Years after the end of the fiscal year.	Secure Shredding / Deletion
Customer Transaction Data	Industry-specific regulations (e.g., GDPR, CCPA, HIPAA)	Defined by specific regulation (e.g., 5-10 Years).	Secure Deletion
Email Communications	Litigation Hold / General Business	3 Years (after employee departure or communication date).	Secure Deletion
System Logs/Audit Trails	Security and Forensics	2 Years.	Secure Deletion
Intellectual Property/R&D	Business/Historical Value	Indefinite (until formally decommissioned).	Migrated to permanent historical archive.

4. Security and Access Control

Data archiving requirements include **access control restrictions to the archived locations** to protect data confidentiality and integrity during its retention period.

1. **Encryption:** All archived data must be **encrypted at rest** using strong, industry-standard cryptographic algorithms. Encryption keys must be securely managed and separated from the archived data itself.
2. **Strict Access Control:** Access to the archive storage (physical or logical) must be restricted via **Role-Based Access Control (RBAC)**. Access is granted only to

personnel who require it for specific, pre-approved tasks (e.g., legal discovery, audit requests).

3. **Audit Trails:** All access attempts to archived data, successful or failed, must be logged and regularly reviewed to detect unauthorized activity.
4. **Segregation:** Archived data must be logically or physically segregated from production and backup environments to prevent corruption or compromise from operational incidents.

5. Roles and Responsibilities

Role	**Responsibility**
Data Owners	Determining the retention period and criticality of the data they own, based on legal counsel and business needs.
IT Operations Team	Executing the archiving process, managing the archive storage infrastructure, and performing secure data deletion when retention periods expire.
Security Team	Reviewing and enforcing encryption, access control, and audit logging for all archived data locations.
Legal/Compliance Team	Providing definitive guidance on mandatory retention periods and initiating legal holds when required.