PREPARED BY: TS SECURITY SOLUTIONS	
ON THE BEHALF OF:	TStephens Information Security Committee
EFFECTIVE DATE:	July 2025
NEXT REVIEW DATE:	July 2026
REVIEW CYCLE:	Annually in July
STATUS:	☒ Working Draft ☐ Approved ☐ Adopted
CONTACT:	teriousstephens@gmail.com

TStephens LLC

Data Retention and Disposal Policy

TS Security Solutions
7-21-2025

Data Retention and Disposal Policy

Purpose

This policy outlines the standards and procedures for retaining and securely disposing of data collected, processed, or stored by TStephens LLC and their clients. The objective is to ensure data is retained only as long as necessary and disposed of properly to protect confidentiality, integrity, and compliance with legal and regulatory obligations.

Audience

This policy applies to all employees, contractors, vendors, and affiliates of TStephens LLC who manage, access, or handle organizational or client data in any form.

Policy

TStephens LLC shall retain data only for the minimum duration required to satisfy legal, regulatory, operational, or contractual obligations. Data that no longer serves a business or compliance purpose must be securely disposed of in a manner that prevents unauthorized recovery or disclosure.

Data Classification and Retention Schedule

Data Classification	Examples	Retention Period	Approved Disposal Method
Public	Press releases, promotional content	2 years	Basic digital or physical deletion
Internal Use Only	Internal project notes, internal memos	3–5 years	Digital wipe, shredding
Confidential	Employee records, internal audits, client contracts	7 years	Encrypted wiping, certified shredding
Regulated	HIPAA, PCI, GLBA, CCPA-related data	Per legal mandate	Degaussing, destruction with proof

Secure Disposal Requirements

- Paper records must be destroyed using cross-cut shredders or sent to an authorized destruction service.
- Digital data must be wiped using DoD-compliant software or equivalent standards.
- Decommissioned storage devices must be destroyed or degaussed prior to disposal.
- Data on cloud platforms must be securely deleted using the provider's verified data sanitization process.

Roles and Responsibilities

- **Information Owners:** Identify applicable retention periods and initiate secure disposal.
- **IT Department:** Execute secure deletion processes and maintain disposal logs.
- **Compliance Officer:** Ensure legal alignment and conduct retention audits.
- **All Staff:** Adhere to this policy and report concerns or incidents involving improper data disposal.

Compliance References

- **NIST SP 800-88 Rev.1: Guidelines for Media Sanitization**
- **ISO/IEC 27001: A.8.3.2, A.11.2.7**
- **GDPR Article 5: Data Minimization & Storage Limitation**
- **HIPAA Security Rule §164.310(d)(2)(i)-(ii)**
- **PCI DSS v4.0: Requirement 3.1**

Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination or legal penalties, depending on the nature and severity of the violation.

Review and Maintenance

This policy will be reviewed annually and updated as necessary to reflect changes in legal requirements, industry best practices, or business operations.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	July 2025		TS Security Solutions	Document Origination