STEWARDS™

DATA RETENTION AND SECURE DISPOSAL POLICY (Safeguards)

STEWARDS, INC.

Approval History

Version	Approved By	Approved On
1.0	Steve Marino	06-09-2024
2.0	**Steve Marino**	**12-04-2025**

Purpose

This policy establishes the requirements and procedures for the secure retention, handling, and disposal of confidential, sensitive, or otherwise protected information owned or controlled by **Stewards, Inc.** (“the Company”).
Its objective is to safeguard Company information throughout its lifecycle and ensure compliance with applicable laws, regulations, and contractual obligations.

Scope

This policy applies to **all Stewards, Inc. employees, contractors, systems, and repositories**, including:

- Physical documents
- Digital files stored on Company-owned devices
- Cloud-based systems and storage environments
- Electronic media (e.g., drives, tapes, disks)

Company information stored in **third-party systems** is subject to the vendor's data disposal policies, which must be **equally or more restrictive** than this policy.

Policy

1. Secure Data Disposal Procedures

A. Physical Print Media

Physical documents containing confidential, sensitive, or protected information shall be destroyed by one or more of the following approved methods:

1. **Cross-Cut Shredding**
    - Documents must be shredded using Company-issued, cross-cut shredders.
2. **Locked Shredding Bins**
    - Employees must deposit materials into locked shredding bins serviced by a **licensed and bonded information-destruction contractor**.
3. **Incineration**
    - Physical destruction performed by a licensed and bonded destruction contractor.

B. Electronic Media

This includes hard drives, solid-state drives, tape cartridges, USB flash drives, CDs/DVDs, printer and copier hard drives, etc.

Approved disposal methods:

1. **Overwriting (Data Sanitization)**
    - Data is replaced using an authorized, sector-by-sector overwriting tool (e.g., Active@ KillDisk).
2. **Degaussing**
    - Strong magnetic fields or electrical degaussing equipment scramble magnetic media into an unrecoverable state.
    - Only NSA-approved degaussers may be used.
3. **Physical Destruction**
    - Media must be fully destroyed (crushing, shredding, pulverizing) to ensure data cannot be extracted or reconstructed.

---

2. Retention of Customer Information

Stewards, Inc. shall retain customer information **no longer than two (2) years after its last use**, unless retention is required for:

- **Legitimate business purposes**
- **Legal, regulatory, or compliance obligations**
- **Operational circumstances** where targeted disposal is not feasible due to system architecture or data structure

The Company shall implement retention procedures to ensure data is not retained beyond required periods.

Enforcement

Violations of this policy may result in:

- Disciplinary action, up to and including **termination of employment**
- **Civil or criminal penalties**, where applicable
- Contract termination for third-party violators

All employees are required to comply with this policy and report suspected violations immediately.