STEWARDS™

INFORMATION SECURITY 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

The purpose of this policy and the **Stewards Information Security Program (ISP)** is to ensure that Stewards, Inc. (“the Company”) information assets that store, transmit, or process Customer Information are properly identified, documented, and protected at all times.
This policy establishes key principles governing the responsible use of Company information and outlines the roles and responsibilities required to maintain the confidentiality, integrity, and availability of Customer Information.

Scope

This policy applies to:

- **Customer Information** in any format
- **Stewards, Inc. information systems** that store, transmit, or process Customer Information
- Systems used, maintained, or hosted by **third-party vendors**
- All **employees, contractors, and authorized users** of Stewards information systems

---

Policy

Policy Statements

Stewards, Inc. has implemented and maintains an Information Security Program (ISP) which includes the following requirements:

- Stewards continuously improves and aligns its information security controls with global best practices.
- Information security policies are reviewed regularly. Employees must acknowledge compliance annually.
- Security awareness training is conducted on a recurring basis.
- Internal assessments or audits of the ISP occur periodically, with findings remediated promptly.
- A documented risk assessment process is maintained and followed.
- Information asset inventories must be updated when new assets are added or existing assets are modified.
- Roles and responsibilities related to information security must be clearly defined and communicated.

- Information must be handled based on its sensitivity, regulatory classification, and contractual requirements.
- Appropriate communication channels are maintained with relevant authorities and security communities.
- An Incident Response Plan (IRP) is established and reviewed at least annually.
- Stewards assesses and manages information security risks related to third-party vendors.
- Change management and vulnerability management controls must be implemented and maintained.

Roles and Responsibilities

Qualified Individual

Stewards, Inc. has appointed a **Qualified Individual** responsible for information and data security, including Customer Information.
This role is overseen by **Ownership** of Stewards, Inc.

Responsibilities include (but are not limited to):

- Implementing and ensuring Company-wide information security
- Approving changes to information security policies
- Monitoring and driving continuous security improvements
- Reporting security risks and program effectiveness to executive leadership
- Advising leadership on industry standards and best practices
- Managing information security communication and training
- Ensuring third-party vendors maintain equivalent safeguards

- Conducting risk assessments and maintaining the risk register
- Partnering with the business to raise security awareness
- Investigating security incidents
- Coordinating and maintaining incident response documentation

---

Information Security Policies

This document, along with all other Company information security policies, defines the principles and requirements of the Stewards ISP and establishes the responsibilities of users and employees.

Risk Assessment

The Company performs an **annual risk assessment** to identify strengths and weaknesses in protecting Customer Information.
Assessments are aligned to the safeguards in **16 CFR 314 (FTC Safeguards Rule)**.

Findings are used to improve the ISP, update safeguards, and revise the risk register.

Safeguards

Stewards has implemented safeguards to ensure the confidentiality, integrity, and availability of Customer Information.

Access Reviews

- Regular access reviews ensure that only authorized users have access to Customer Information.
- Users must have the **minimum access necessary** to perform their duties.
- Reviews are documented in a Governance, Risk & Compliance (GRC) system.

Asset Inventories

The Company inventories all assets that store, transmit, or process Customer Information, including:

Personnel

Human Resources maintains a current list of users and third parties who may access Customer Information.

Devices

The Qualified Individual maintains an inventory of all hardware devices, including desktops, laptops, network gear, mobile devices, servers, etc.

The inventory includes:
Name, Type, Description, Manufacturer, Model, OS, IP, MAC, Location, Purchase Date, Support/Warranty, etc.
Device status is maintained in the IT provider's EDR tool.

Systems (Software and Applications)

The Qualified Individual maintains a systems inventory which includes:

- System type and deployment method
- Data types processed or stored
- User and third-party access
- Licensing information

- Encryption details
- Logging and monitoring details
- MFA status
- Security evaluations or vendor ISP links

Facilities

The Business Office maintains a list of facilities, including physical security controls (CCTV, card access, etc.) relevant to secure Customer Information storage.

Encryption

- Encryption at rest and in transit is required for systems storing or transmitting Customer Information.
- Encryption status is documented in asset inventories.

Application Security

- Information systems storing or processing Customer Information are subject to security evaluation.
- Stewards acquires software from vendors that maintain security programs or application security assessments.

Multifactor Authentication (MFA)

- MFA is required for all information systems where supported.
- Systems lacking MFA must be upgraded, replaced, or assigned equivalent compensating controls.

Secure Disposal of Customer Information

Stewards has implemented a Secure Disposal Policy ensuring:

- Protected information is destroyed securely
- Customer Information not associated with an active relationship is disposed of no later than **2 years after last use**

Change Management

A formal Change Management Policy governs updates to systems storing or processing Customer Information.

Monitoring and Logging

- The Company monitors user activity and implements methods for detecting unauthorized access.
- Logging or alerting is enabled for all systems that support it.
- Systems lacking such capabilities must be replaced or supplemented.
- Logs are reviewed periodically to identify unauthorized activity.

ISP Testing and Monitoring

- Key safeguards and controls are regularly monitored and tested.
- A cybersecurity firm conducts annual penetration tests and periodic vulnerability scanning.
- The Qualified Individual updates the ISP based on system changes, testing results, and risk assessments.
- The ISP is reviewed annually for effectiveness.

Security Awareness and Training

- Annual information security training is required for all personnel with access to Customer Information.
- A cybersecurity firm conducts phishing simulations.
- The Qualified Individual monitors advisories from CISA NCAS for emerging threats.

Service Provider & Vendor Risk Management

- The Company maintains an inventory of service providers with system or Customer Information access.
- All such providers must maintain an ISP with safeguards at least equivalent to Stewards' ISP.
- Vendors lacking adequate safeguards must become compliant or be replaced.

- Vendors are reviewed annually for compliance and adequacy.

Incident Response Plan (IRP)

Stewards maintains an IRP designed to rapidly respond to and recover from incidents affecting the confidentiality, integrity, or availability of Customer Information.

Enforcement

Violations of this policy may result in:

- Disciplinary action up to and including termination
- Civil or criminal penalties

All employees, contractors, and third-party users are required to comply with this policy.