STEWARDS™

INCIDENT RESPONSE PLAN (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 Incident Response Plan (IRP) provides procedures and guidance for identifying, reporting, analyzing, responding to, and recovering from information security incidents across the **Stewards, Inc.** systems environment.
Its purpose is to minimize operational, legal, and reputational impact by ensuring a structured and timely response to threats affecting Customer Information or Company systems.

Scope

A **security incident** or **security breach** is defined as an occurrence in which computer security controls fail to prevent any of the following:

- **Unauthorized access or use** of computer systems, including unauthorized use resulting from compromised credentials
- **Denial-of-service (DoS) attacks**
- **Malicious code infections**, including viruses, Trojans, worms, ransomware, or spyware
- **Any event causing significant negative impact** to the confidentiality, integrity, or availability of systems or data that Stewards stores, processes, or transmits

This Plan applies to all Stewards employees, contractors, and third parties authorized to use Company information systems.

IDENTIFYING A SECURITY INCIDENT

All users—including employees, contractors, and third parties—are responsible for identifying and reporting suspicious activity that may indicate a security incident.

Common indicators include:

- Password changes you did **not** initiate
- Inability to log in or sudden account lockouts
- Unfamiliar browser home pages or persistent pop-up ads
- New desktop icons appearing unexpectedly
- Malware infections or antivirus alerts
- Sudden workstation slowdowns or high CPU/network activity
- Unexplained file modifications, deletions, or additions
- Rapid decrease in available hard drive space

Many incidents require technical analysis to confirm impact and scope.

PRIOR TO REPORTING AN INCIDENT

Upon discovering a potential or actual incident:

1. **If credentials are compromised**, immediately change the password and report the incident.

2. **If a device is affected**, stop working, save files if possible, close applications, and **shut down the device**.

3. Do **not** resume use until cleared by IT support.

4. Do **not** discuss the incident with anyone except authorized Stewards personnel or approved IT support.

This prevents tampering and limits misinformation.

REPORTING AN INCIDENT

All potential or actual security incidents must be reported **immediately**.

Reports should be made to the:

- **Qualified Individual**

- **Designated IT support personnel**

A valid report must include, at minimum:

- Date and time of the incident

- Type of incident

- Detailed description of what occurred

- Location of the affected system

- Contact information of the reporter

Prompt reporting ensures rapid containment.

HANDLING AN INCIDENT

Upon receiving a report, the Qualified Individual or designated personnel will initiate response activities **immediately**, and no later than **60 days** from the initial report.

If Customer Information is impacted:

- The Qualified Individual must contact the Company's **cyber insurance carrier immediately**.
- The carrier will assign a **breach coach** to guide Stewards through legal, forensic, and communication requirements.
- Only approved vendors may conduct forensic investigations or notifications.

Documentation Requirements:

The Qualified Individual must document:

- Timeline of events
- Incident details
- Actions taken
- Notifications made
- Root cause analysis
- Recommended prevention measures

If the incident affects multiple organizations or requires law enforcement attention, it must be reported promptly to:

- **US-CERT**

- Appropriate law enforcement agencies

ROLES AND RESPONSIBILITIES

Users (Employees, Vendors, Contractors, Clients)

Responsibilities include:

- Reporting incidents as soon as possible
- Taking detailed notes and providing accurate information
- Cooperating with IT, the Qualified Individual, and investigators

---

Qualified Individual / Information Security Officer

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

Responsibilities include:

- Overall responsibility for implementing and enforcing information security across the Company
- Approving changes to security policies
- Monitoring continuous improvements and recommending updates
- Reporting security risks and program effectiveness to executive leadership and the Board
- Advising executive leadership on security standards and best practices
- Communicating security policies and awareness programs

- Coordinating risk management efforts across departments
- Ensuring third-party vendors maintain adequate safeguards
- Overseeing incident response and coordinating communication requirements
- Maintaining incident documentation and ensuring proper retention

---

Enforcement

Violations of this policy—including failure to report incidents, improper handling of evidence, or unauthorized disclosure—may result in:

- Disciplinary action
- Termination
- Civil or criminal penalties

All personnel must comply with this policy and support a secure incident response process.