



# ORGANIZATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES (Safeguards)

STEWARDS, INC.

---

## Approval History

Version	Approved By	Approved On
1.0	Steve Marino	06-09-2024
2.0	<b>Steve Marino</b>	<b>12-04-2025</b>

---

The table below describes the roles and responsibilities established to fulfill the Company's information security, privacy, and operational safeguard obligations.

These definitions ensure clear communication of security policies and standards, assign ownership, and promote coordinated implementation across departments.

They serve to clarify how information protection is governed, executed, and maintained throughout the organization.

---

## Roles & Responsibilities

### Executive Leadership (CEO, COO, and other CXO Roles)

- Approves capital expenditures for Information Security
- Communicates Information Security priorities to senior management and ownership
- Receives and reviews the annual Information Security Report
- Consults with senior leadership to understand mission and risk, ensuring alignment
- Aligns Information Security policy and posture with the Company's mission and objectives

---

## **Qualified Individual**

- Reports information security risks annually to executive leadership and obtains approval for required remediation
- Develops and maintains Information Security policies and standards
- Establishes information security frameworks and awareness programs
- Serves as security liaison to the Board of Directors, law enforcement, auditors, and legal counsel
- Conducts risk assessments, documents threats, and maintains the risk register
- Assists departments, projects, and programs with data classification and required controls
- Develops policies, standards, processes, and solutions to mitigate identified risks
- Works with IT resources to embed security frameworks into operations
- Monitors infrastructure and data repositories for malicious activity
- Investigates security incidents
- Provides information security consulting across the Company
- Provides oversight and direction for privacy requirements relating to Protected Health Information (PHI) and Protected Individual Information (PII)

- Manages and coordinates incident response, communication, and notification
- Maintains incident documentation and oversees documentation retention activities

---

## **System Owners**

- Manage confidentiality, integrity, and availability of information systems under their control
- Develop and implement access management processes for their systems
- Ensure compliance with information security and privacy policies
- Advise the Qualified Individual on financial resources required for systems and controls
- Maintain system documentation and ensure application of required security controls
- Carry out additional responsibilities delegated by the Qualified Individual

---

## **Employees and Contractors**

- Act in a manner that protects the health, safety, and security of themselves, coworkers, and the information resources they access
- Help identify areas where additional risk management practices are needed
- Take practical steps to reduce exposure to liability
- Follow all guidance from the Qualified Individual, IT resources, and mandatory security awareness training
- Report any unusual or suspicious activity to the Qualified Individual or IT resources