STEWARDS™

CHANGE MANAGEMENT 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 management direction, requirements, and high-level objectives for the Change Management process at **Stewards, Inc.** Its purpose is to ensure that changes to information systems are implemented in a controlled and secure manner to reduce risks such as:

- Corruption or destruction of information
- Adverse impacts on business processes
- System performance degradation

- Service disruption or productivity loss

Scope

This policy applies to all **Stewards, Inc.** IT systems and applications that store, process, or transmit information, including:

- Servers, network devices, and computer hardware
- Software, cloud applications, and on-premise systems
- Mobile devices and telecommunications systems
- Any business unit utilizing Company information systems

Policy

All changes to information resources must be managed under a formal **Change Control Process**. This ensures changes are properly reviewed, approved, tested, documented, implemented, and monitored.

Policy Requirements

Stewards, Inc. shall:

- Maintain a **baseline configuration standard** for all systems and update it with each system change or component installation.
- Require **all change requests** to be logged in the ticketing system of record, including approvals, notes, testing results, and implementation details.
- Ensure **all changes are authorized, documented, and controlled** using approved procedures.
- Monitor configuration changes across systems.

- Require **testing and peer review** prior to deployment into production.
- Use automated tools, when available, to support change initiation, tracking, approval, and documentation.
- Classify urgent service-restoration changes as **Emergency Changes**.
- Classify routine, low-risk actions as **Standard Changes**.
- Notify customers in advance when changes may affect them.
- Maintain strict **environment separation** (development, test, production).
- Prohibit the use of **production data** in development or testing.
- Require removal of test accounts and test data before systems go live.
- Maintain documented procedures for security patches and software updates.

Change Initiation and Impact Analysis

All scheduled and unscheduled changes must be documented and tracked.

Documentation must include:

- Scope of the change
- Areas and systems affected
- Back-out / rollback procedure
- Test plan
- Communication plan
- Deployment date

Impact analysis must evaluate:

- Business risks
- Technical and operational risks
- Security implications
- Associated costs

Each change must include a complete **implementation plan** and **rollback strategy**.

Change Approval and Implementation

- Changes must receive **formal approval** before development and before deployment to production.
- Cross-departmental impact must be reviewed when the change affects multiple business services.

Post-Implementation Review

A review shall be conducted to confirm that:

- The change achieved its intended result
- No unintended consequences occurred

If stability issues arise, the change may be rolled back at the discretion of the change review team.

Denials

The Business Owner or designee may deny a change for reasons including:

- Insufficient planning or testing
- Lack of stakeholder approval
- Integration concerns
- Missing rollback plan
- Security risks
- Poor timing relative to business operations
- Conflict with resource availability (late nights, weekends, holidays, major events)

Emergency Changes

Emergency changes:

- Are used only when regular processes cannot be followed
- Require immediate implementation to avoid business disruption
- Must be verbally authorized by an appropriate service manager
- Must be **retrospectively documented and approved**
- Must be reviewed during scheduled CAB/Business Owner meetings for:
    - Root cause
    - Lessons learned
    - Impact
    - Prevention measures

Standard Changes & Patching

Standard (pre-approved, low-risk) changes—such as applying security patches—may be performed without the full approval workflow, but still require ticket documentation.

The Company shall:

- Patch all systems regularly and in accordance with documented timelines
- Use **CVSS scoring** to prioritize patching
- Identify systems affected by software or firmware vulnerabilities
- Notify designated personnel of relevant patches or threats
- Address vulnerabilities discovered through:
    - Assessments
    - Monitoring
    - Incident response
    - Error handling

Enforcement

Violations of this policy may result in:

- Disciplinary action
- Termination
- Civil or criminal penalties

All employees and contractors must follow the Change Management process without exception.