Change Management Policy

Version 3.0

12th February 2020

Rue des Oursins, 21731, Baie du Tombeau I T : +(230) 206 8200 I F : +(230) 247 1010 I E : corporate@lasentinelle.mu

Document History

Created by:	Eddy Lareine
Approved by:	Areff Salauroo

Release date	Version	Change Details	Reviewed by
22.10.19	1.0	Submitted for review	Legal Advisor
12.11.19	2.0	Apply changes submitted by legal advisor	Eddy Lareine
12.02.20	3.0	Submitted for review	Areff Salauroo

Table of Contents

Table of Figures

CHANGE MANAGEMENT POLICY

1.0 Objective

The purpose of this policy is to ensure that changes to information processing facilities and systems are controlled and changes to the provision of third-party services are managed.

2.0 Scope

This policy applies to employees, contractors and Third Parties of La Sentinelle Ltd.

3.0 References to ISO 27001:2013

- **Change Management - A.12.1.2**
  Changes to the organization, business processes and information processing facilities and systems shall be controlled.

- **Managing Changes to Supplier Services - A.15.2.2**
  Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls shall be managed, taking into account of the criticality of the business information and processes involved and the re-assessment of the risks.

- **System Change Control Procedures - A.14.2.2**
  Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

4.0 Policy Description

Due to the criticality of La Sentinelle Ltd information systems and sensitivity of information, it is important to control the implementation of changes by the use of formal change control procedures so as to maintain the security, integrity and availability of application system software and information.

4.1 Change Management Business Process Flow

Changes to information processing facilities and systems are controlled and operational systems & application software are subject to strict change management control, as per "Change Management Process Flow 1.0" below.

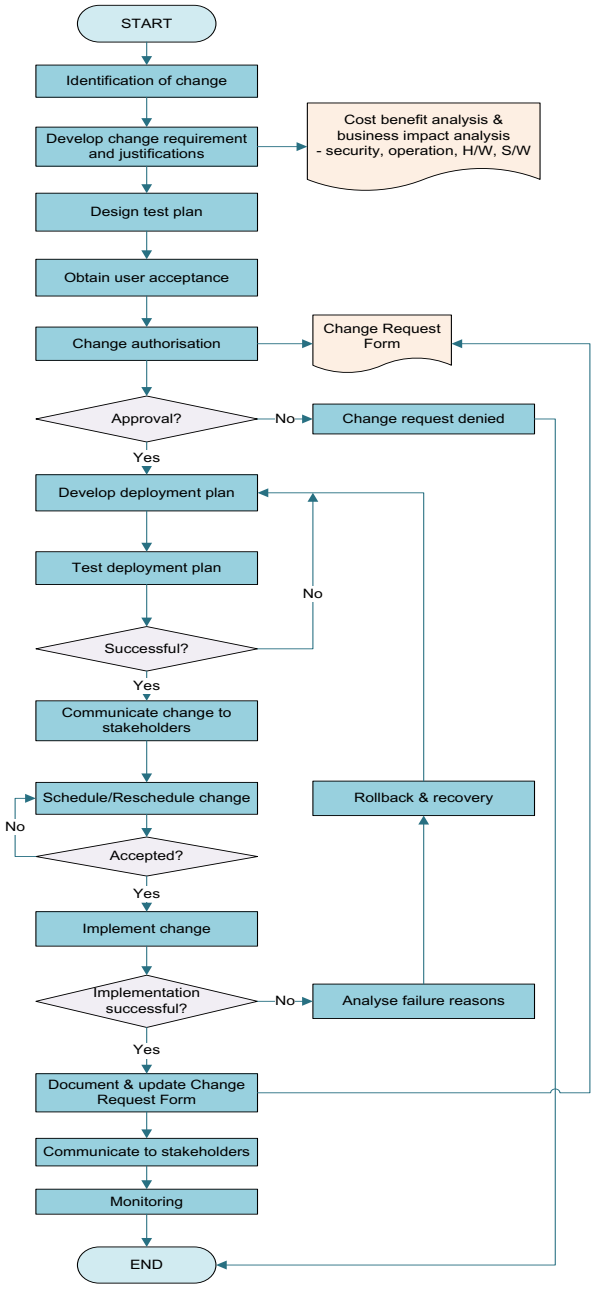

Figure 1 - Change Management Process Flow 1.0

4.2 Managing Changes to Supplier Services

Changes to the provision of services, including maintaining and improving existing information, security policies, procedures and controls, are subject to a formal management process.

A reassessment of risk is undertaken to ensure that the new requirements are covered by existing contracts, policies, procedures and controls and also takes into account the criticality of the particular business systems and business processes.

The following are taken into account in the process of managing changes to a Supplier Service: -

- Changes made by the organization to implement: -

    1. *Enhancements to the current services offered;*
    2. *Development of any new applications and systems;*
    3. *Modifications or updates of La Sentinelle Ltd's policies and procedures;*
    4. *New controls to resolve information security incidents and to improve security*.

- Changes in their service level agreement to implement: -

    1. *Changes and enhancements to networks, systems and information processing facilities;*
    2. *Use of new technologies;*
    3. *Adoption of new products or new versions/releases;*
    4. *New development tools and environments;*
    5. *Changes to physical location of service facilities;*
    6. *Change of suppliers;*

4.3 Change Control Procedures

Change control procedures are documented and enforced in order to minimize the risk of corruption of information systems. Whenever new systems are implemented or changes are brought to existing systems, the following procedures are ensured:

i. A request for implementation of a new system or for changes to an existing system is submitted to La Sentinelle Ltd IT Management for authorization. Whenever appropriate, relevant documentation and specifications are attached to the request. Documentation includes risk assessment and business impact analysis.

ii. La Sentinelle Ltd IT Management analyzes the request and accompanied documentation and approves or rejects the request. In case the request is approved, a project plan is initiated whenever applicable. Responsibilities for carrying implementation or changes are clearly defined.

iii. Equipment, software, information and database that require amendments are identified.

iv. A testing plan is implemented and tests are formally recorded.

v. System documentation is updated after changes are implemented. Version controls and change requests audit trails are maintained.

vi. Documentation and user procedures are updated to reflect changes.

It is ensured that implementation of changes are carefully planned in order to avoid disturbance of normal business activities.

4.4 Emergency Change Management

Formal emergency change processes are followed to allow for a high-priority change to flow through quickly. Standard change management process may require more time than what is realistic. During emergency change processes, La Sentinelle Ltd IT Department/Management will ensure that risks are properly managed by establishing a certain degree of review prior to implementation and a full review at a later point.

Whenever an emergency change is identified, the La Sentinelle Ltd Senior Management Team will be notified and reasons for emergency change will be specified by the requestor. The change will be reviewed and authorized by the General Manager before it goes on production. Emergency change process will be for exceptions and it must be ensured that it does not become a shortcut to getting changes into production for whatever reason.

Once the emergency change has been implemented, the responsible party or parties will generate a formal Change Request Form and document the results for the IT Management team to review. The guidelines below are used any emergency change management:

i. The IT Management Team will need to understand the change in order to communicate it to others who may question the reasons for an emergency change.

ii. The IT Management Team needs to review the change and make sure it doesn't affect other changes that may be in process, future direction, etc.

iii. There needs to be an understanding of lessons learned, for example how this type of emergency could be prevented or better handled in the future.

iv. The IT Management Team needs to ensure the change was of an emergency nature. Else, a corrective action will be needed.

v. Formal documentation will ensure knowledge of the production environment in order to support the configuration, release, incident and problem management processes.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Employee Declaration

I have read and I understand the above Change Management Policy, and consent to adhere to the rules outlined therein.

Name : _____

Signature : _____

Date : _____

Annex 1 - Change Request Form

Requested by:		**Customer Reference (optional):**
Level of Urgency:	**(1. Immediate 2. ASAP 3. Anytime)**	**Requested Date: ___/___/___**
Change Requested: **(if any)**	**Related Problem Report number/Test Form Number:**	
Authorised: _____ **(This is not a commitment to implement the change)**		**Date: ___/___/___**
		Change Request No:
Project:	**Project Code:**	**Version No:**
Estimated Effort (Md):	**Estimated Cost:**	
Engineering Change Proposal Required & Attached: Yes / No		
Rework/Retesting/Reviews/Acceptances Required: **Identify The Specific Products, Inspections Or Reviews And Tests And Sign Off When Done** **Requirements | Design | Programming | Test Specs | Testing | Rollback Plan | Documentation | Other (Specify) |** **Current version:** **New version:**		
Approved Implementation Estimate: _____ **(Line Manager)**		**Date ___/___/___**

Acceptance & Authorisation To Implement (This Is A Commitment To Implement The Change):

Accepted: _____ **Date** ___/___/___
(Customer/Originator)

Authorised: _____ **Date** ___/___/___
(Line Manager)

Helpdesk Ticket Number:

Rollback Section
Description Of Rollback Procedure (Indicate Version/Access Path)
Implementation Section
Description Of Change (Indicate Programs/Network/Equipment Affected)
Assign To: **Commencement Date:** ___/___/___
Sign When Done: **Completion Date:** ___/___/___

Retesting By: **Date: ___/___/___** **(Please Attach Test Documentation)**
User Acceptance (This Is A Commitment From Customer/Originator That Change Has Been Implemented To His Satisfaction): **Accepted: _____** **Date ___/___/___** **(Customer/Originator)** **Closed Out By: _____** **Date ___/___/___** **(Line Manager)**

Annex 1 - Change Request Form