




# Change Management Process


Doc. Control Number	Version
SNL-33	0.2



## Document Reference

Item	Description
Title	Change Management Process
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	28 May 2023
Revision-Date	28 May 2024

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/28/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/28/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/28/2024 

## Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	28 May 2023	Muhaned Ali	First Release
0.2	28 May 2024	Muhaned Ali	The document has been reviewed



## Contents

1. Purpose.....	4
2. Scope .....	4
3. Change Management Process .....	4

## 1. Purpose

To maintain integrity, security, and availability of IT systems at SNLC there needs to be a robust and mandatory Change Management policy in place to control the required amendments, enhancements and changes to existing systems and services, as well as the introduction of new services.

## 2. Scope

This applies to ALL changes, new services, additions, or amendments to any system or service managed by SNLC, including patching, configuration changes, upgrading, and new equipment.

## 3. Change Management Process

1. Create & Log the Request for Change (RFC)
 

A Request for change is created by the change requester, requiring the change. All normal changes will be sent via email and submitted to the CAB for Review.
2. Review Request for Change (RFC)
 

Each Request for Change should be reviewed and prioritized by the Change Manager. These RFCs should be queried with the Change Requester esp. if it requires more detail/ clarity around the implementation plan/ backout plan/ any process changes required/ additional documentation around KIs. These changes will be monitored by the Change Manager and once satisfactory responses have been received and input into the RFC for an audit trail, it will be scheduled in for the CAB Review.
3. Evaluate the Change (RFC)
 

Evaluating the change to assess the impact, risk and benefits to IT services is critical to avoid unnecessary disruption to business operations at SNLC. Impact assessment will consider the impact/ risk of the Change presented and reviewed by the CAB around the business, infrastructure, customers, implementation resources and currently scheduled changes in the change log. The CAB will consist of various ITS stakeholders at SNLC such as the Head of Systems, Head of Networks, Head of Security, Web Team Manager, and the Helpdesk Manager who will be responsible for evaluating the Change.
4. Approve/Authorize the Change (RFC)
 

Change requests commonly require authorization prior to implementation (except in the case of retrospective Emergency Changes) and each change requires authorization from the CAB to proceed. In the case of Emergency Changes which are logged for urgent approval, the Change Implementer will notify the Change Manager/ Team Manager of it. It will need at least one member of CAB to sign off an Emergency Change.
5. Coordinate Implementation
 

Once authorized, the Change is handed over to the release and deployment process for coordination and collaboration with the appropriate technical management teams for building, testing, and deploying the change. Each change should have remediation plans prepared in case of an implementation failure. The Change Calendar will be kept up to date with all upcoming changes that may impact on them. The Change Calendar along with any expected deviations in service availability will need to be taken into consideration when coordinating change implementation.
6. Review and Close Change Request
 

Upon completion of the Change, a Post Implementation Review (PIR), which is a review of the detail implementation results and lessons learnt, will need to take place if there were deviations to the expected outcome of the Change.