




Change Management Policy

Doc. Control Number	Version
SNL-14	0.3



Document Reference

Item	Description
Title	Change Management Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	13 March 2024
Revision-Date	13 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	13/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	13/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	13/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	23 May 2022	Muhaned Ali	First Release
0.2	23 May 2023	Muhaned Ali	The policy has been reviewed
0.3	13 March 2024	Muhaned Ali	The policy has been reviewed



Contents

1. Purpose And Overview	4
2. Scope.....	4
3. Policy.....	4
4. Policy Compliance	8

1. Purpose And Overview

To maintain the 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.

This policy sets out the process and procedure for this IT Service Change Management requirement.

2. Scope

ALL changes, new services, enhancements, or amendments to ANY system or service which SNLC manages, including cloud services must go through the Change Procedure.

3. Policy

3.1 Definition of a Change

SNLC IT Services defines a change as anything that alters, modifies, or transforms the operating environment or standard operating procedures of any systems or services that have the potential to affect the stability and reliability of infrastructure or disrupt the business of SNLC.

Changes may be required for many reasons, including, but not limited to:

- User requests.
- Vendor recommended/required changes.
- Changes in regulations.
- Hardware and/or software upgrades.
- Hardware or software failures.
- Changes or modifications to the infrastructure.
- Environmental changes (electrical, air conditioning, data center, etc.).
- Unforeseen events.
- Periodic Maintenance.

3.2 Policy Definition

It is the responsibility of IT Services to manage the lifecycle of all systems supporting SNLC business and technical objectives.

There are two categories of changes that are permitted. They can either be Pre-approved or Change Advisory Board (CAB) approved and of these categories, there are four types:

Minor/Routine, Major/Significant, Emergency/Unscheduled, and New Development.

3.3 IT Assets

This policy covers the data networks, local servers, and personal computers (stand-alone or network-enabled), located at the KHB office, RIY office, KHB HUB, and Mediacom office, and any personal computers, laptops, mobile devices, and servers authorized to access the organization's data networks.

3.4 Change Management process

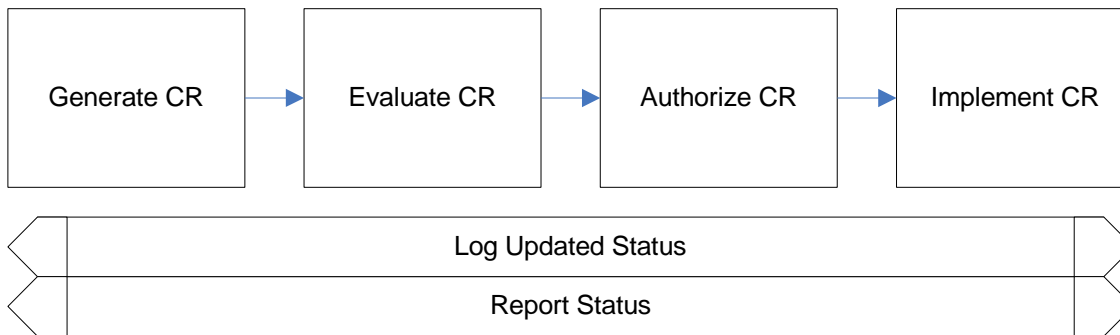
All Changes to live services will be carried out under the jurisdiction of the Change Management Process. This includes both Operational and Project (newly introduced Service) Changes.

3.5 Change Request Process Flow Requirements

The following outlines a generic change request process flow:



Step	Description
Generate CR	A submitter completes a CR Form and sends the completed form to the Change Manager
Log CR Status	The Change Manager enters the CR into the CR Log. The CR's status is updated throughout the CR process as needed.
Evaluate CR	Project personnel review the CR and provide an estimated level of effort to process, and develop a proposed solution for the suggested change
Authorize	Approval to move forward with incorporating the suggested change into the project/product
Implement	If approved, make the necessary adjustments to carry out the requested change and communicate CR status to the submitter and other stakeholders



3.6 Roles

Roles	Description
Change Requestor	Anyone who wants to raise a request for change (RFC)
Change Owner	The person who ensures the assessment, prioritization, scheduling communication, and delivery of the change
Change Implementer	The person who creates, builds, tests, and deploys the change
Change Management Process Manager	The person who administers the change process, ensuring all necessary process steps are completed and improvements are raised, when necessary
Change Approver	The person/group who approves the change(s)
CAB (Change Advisory Board) / ECAB (Emergency Change Advisory Board)	The group/body that exists to support the authorization of change and to assist Change Management in the assessment, prioritization, and scheduling of change, resolving priority conflicts.

3.7 Change types

Change Type	Definition	Technical Approval prior to CAB	CAB Submission Deadline
Standard	A routine change that is low risk, relatively common, and follows a pre-defined procedure. Customer approval is still required. For a normal change to be upgraded to a standard change, it must have been completed successfully three times as a normal change and the procedure	No	No

	documented. The creation of the standard template requires approval by the change manager.		
Normal	A change to an existing service, system, application, or infrastructure component with a potential impact may require CAB approval before being implemented.	Yes	3 hours before CAB for high-risk changes only
Emergency	A change that must be implemented as soon as possible, for example, to resolve a major Incident, implement a security patch, or prevent an imminent failure.	Yes	Emergency CAB required

3.8 Change risks and impact

- Change Risks

When assessing a change, a risk assessment is undertaken using the following criteria:

1- High:

- Previous change has been made and was not successful
- Complex implementation or back-out plans
- New technology, not previously implemented

2- Medium:

- Previous similar changes have occasionally been problematic
- Some complexity to implementation or back-out plans
- Standard technology utilized in a non-standard application

3- Low:

- Previous similar changes have always been successful
- Simple implementation or back-out plans
- Standard technology used in a BAU context

- Customer impact analysis

When assessing a change, an impact assessment is undertaken using the following criteria:

1- High:

- The proposed change poses a significant impact on the customer(s) or internal systems in the form of loss of service or serious performance degradation for an extended period.
- Multiple customers or internal departments suffer loss or degraded service during the change window.

2- Medium:

- The proposed change poses an impact on the customer(s) or internal systems in the form of reduced resiliency, redundancy, or capacity.
- A single customer or internal department suffers loss or degraded service during the change window.

3- Low:

- The proposed change has no impact on the customer(s) or internal system systems.

3.9 Changed approval

For each change type the following approval matrix needs to be adhered to:

Change Type	Technical Approval	Customer	CAB / ECAB
Standard	No	Yes	No
Normal	Yes	Yes	Risk Related
Emergency	Yes	Yes	Yes

1- Technical approval

- Technical approval must be given by a higher skilled engineer or peer (of the technology/technologies related to the change) of the engineer implementing the change.
- If the engineering planning and implementing the change has no reviewer of an equivalent or higher skillset, then the change must be set as high risk and assessed by the CAB / ECAB.
- 2- Customer approval
 - Individual customer approval (for changes related to one customer only) must only be accepted by an authorized customer representative.
- 3- CAB / ECAB approval
 - All Emergency changes are to be reviewed by the CAB / ECAB, where they will be approved or rejected. This is in addition to technical and customer approval.
- 4- Emergency
 - A change in response to a major incident where the remedy requires immediate action and will be approved by the Major Incident Manager with evidence of retrospective approval from the customer is requested as soon as reasonably practicable.

3.10 Implementation and testing

1- Change implementation

- All changes should be carried out as described in the RFC and within the designated planned times. If a variation is identified during the change, then this must be presented to either a member of the Change Management team or the Duty Manager to approve the variation. This variation must be documented in the change notes.
- If the variation is not approved, this will result in the change being backed out. This change will then need to be re-planned and re-raised.

2- Testing and validation

- Following the implementation of the change, tests in line with the testing plan set out in the change must be carried out to ensure that the desired result has been verified.
- If a change has not met the acceptance criteria, then the back-out plan must be invoked, as detailed in the RFC.

3- Change completion

- Once the change has been tested and validated, the changing status is changed to completed.

4- Post-implementation review (PIR)

- A change review should be carried out to confirm that the change has met its objectives and that the change initiator and stakeholders are happy with the objectives, and that there have been no unexpected side effects.
- Spot checking of changes rather than large-scale PIRs is acceptable for successful changes, however, a PIR is mandated for changes that have been rolled back, led to unexpected service impact, or changes where there was a variation during implementation.

5- Change closure

- Once the change owner has satisfied themselves all stages of the change life cycle have been completed, and the change can be closed.

3.11 Customer Notification

1- Notification Notice Period

- For planned changes that may cause an outage or serious performance degradation for multiple customers, notifications must be issued at least 5 days in advance. In emergency situations, the 5-day notice period may be waived.



4. Policy Compliance

4.1 Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

4.3 Non-Compliance

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