Change Management Procedure

Procedure

Document ID: SCEE-BS-IT-PRO-0004

Authority

	Title	Name	Date
Owner	HSEQ Manager	Anthony Gollan	14/06/2023
Reviewer	ICT Manager	Imre Szabo-Dobozy	14/06/2023
Approver	SCEE GM Telecommunications	John Prichard	14/06/2023

History

Revision	Date	Amended By (Name)	Details of Amendment
A	19/05/2021	Imre Szabo-Dobozy	Draft created
0.0	09/11/2021	Jackie Alfonso	Issued for Use
1.0	14/06/2023	Arianne Ramirez	Updated to SCEE Electrical

Table of Contents

1 Purpose

The purpose of Change Management Procedure is to define the process for carrying out changes to ICT systems and networks in order to reduce the potential for interruptions of the business operational activities Southern Cross Electrical Engineering (SCEE).

2 Scope

This procedure shall apply to all changes made to any SCEE information systems including, but not limited to, applications, network, platforms, databases, computing facilities, and configurations wherever there is a potential impact to the Information and Communications Technology environment of SCEE.

3 Definitions

Term	Definition
Change	To transform, alter, or modify information systems and networks including physical changes and configuration changes.
Change Advisory Board (CAB)	Group of senior Business and Information Technology team members who validate and approve/reject requests for change (RFC's).
Emergency change	Changes that need to be executed in an urgent timeframe due to the criticality of the implementation requirement.
Impact analysis	Identifying the potential consequences of a change from both a positive and a negative perspective.
Information asset owner	The individual who has been allocated accountability for an information asset(s).
Pre-approved changes	Also referred to as Standard Changes. Changes which occur on a regular basis and are deemed to pose a low risk. These changes must have initially been approved through the CAB process.
RFC	Request for Change, A submission to the CAB requesting that a change take place including all necessary supporting information necessary for the CAB to make their determination. Submitted on a standard form (See Appendix A).
Rollback Plan	A plan, included with the RFC defining how the change will be reversed should an adverse reaction to the change be identified during the implementation.

4 Responsibilities

Role	Responsibility
CAB	Responsible for the approval or rejection of changes.
ICT Manager	Ensures that all Information Technology team members are aware of and follow this procedure.
ICT Team	Adheres to the requirements of this procedure.
Information asset owner	Responsible for submitting requests for changes to their assets and for being part of the CAB in the change approval process

5 Procedure

5.1 Change Advisory Board (CAB)

The CAB will meet fortnightly (in person or virtually) and will consist of the following appointments:

- Manager, ICT (Chair)
- System Administrator
- Information Asset Owner (Business Owner) where applicable
- Person requesting change
- Others as requested by the chair e.g. third-party support providers

The Chair may elect to postpone meetings if no changes are scheduled before the following scheduled CAB meeting.

5.2 Change Request

All changes must be initiated using an approved change request form (Refer to Appendix A Change Request Form (RFC)). The change request form must be completed and sent to the CAB at least two business days prior to the scheduled CAB meeting.

In the event that the change is not initiated from within the Information Technology team, the request is to be approved by the requestors business unit Manager before being submitted to the CAB.

A change request register must be maintained by the Information Technology team to record all requests raised and should capture all relevant information.

For a change request to be valid it must contain a rollback plan that has been tested in a development or test environment.

The Change Advisory Board (CAB) must validate the justification for the change and if accepted, assign and initiate impact analysis and action plan creation for the change request.

CAB members are to receive details of proposed changes (forward schedule of changes) at least one working days prior to the CAB meeting.

5.3 CAB Actions

Upon submission the change request must be analysed by the CAB to identify the impact of proposed change on the information systems environment of SCEE.

The impact analysis must include identification of information systems and users impacted by the proposed change and level of impact on them.

Identify resources required for proposed change, estimated effort, timelines and cost involved in carrying out change.

An action plan must be prepared detailing the activity owner, activities and the schedule for the proposed implementation of changes.

5.4 CAB Approval

The CAB members are to have read and understood changes prior to the CAB meeting.

The CAB Chair has the power of veto over a change, should they believe that the change will be detrimental to the security of or operation of SCEE business. A business-based justification is to be provided where a veto is applied.

Following receipt of approvals from asset owners and relevant business functions, including approval of Impact analysis and Action plans, the change request must be approved by the CAB before it can be formally scheduled.

Approval of a change must include approval of the change window or schedule for when the change will be implemented.

5.5 Emergency Change Process

Where a change is considered to be an emergency change (impact prevents the change waiting for the next CAB meeting) then the following emergency change process is to be actioned:

- An emergency change must be submitted on an RFC form (Appendix A).
- A change deemed to be an emergency change must be approved by the ICT Manager (or delegate) plus one other permanent CAB member before it can be implemented.
- The ICT Manager will assess the quality and accuracy of the information within the RFC and may ask for more information prior to progression.
- The CAB Chair will communicate with all CAB members about the emergency change via email or in a meeting environment (if time permits). The CAB will be required to review and assess the change.
- If an Emergency CAB meeting is held, approval will be captured by the ICT Manager.
- If email approval is sought, all correspondence to the RFC will be visible as a note within the record.
- The ICT Manager will review the approvals for any CAB concerns and progress the RFC for implementation once all concerns have been alleviated.
- Once a change has been approved for implementation, the ‘implement change procedure’ is followed.
- Emergency changes must be retrospectively presented to the full CAB at their next meeting with justification for the designation of ‘Emergency Change’. The change will be presented including a post implementation report (PIR) detailing any issues or consequences of the change.

5.6 Testing, user acceptance and post-implementation

All changes must be tested in a development or test environment prior to implementation on the production environment.

In the event that changes require the training of users, as identified during impact analysis, all affected users must be trained before implementation of change in the production environment.

5.7 Implementation Change

With relevant approvals in place (and documented), the Change Request can be implemented following the approved action plan and on the approved date and time.

Systems and networks must be backed up with snapshots taken, prior to any change being implemented.

All impacted users as identified during impact analysis must be informed about any outage during implementation.

If necessary, due to issues being encountered during implementation, the rollback plan may need to be implemented to ensure that there is no prolonged outage of SCEE operational capability.

Change progress is to be documented.

5.8 Post-implementation

Once implementation has been performed user acceptance must be gauged.

All aspects of the change implementation must be documented including any foreseen or unforeseen issues/impacts arising and the success/failure of the change. This must be presented to the next CAB meeting.

Where necessary, as-built documentation, network diagrams and configuration management documentation are to be updated to accurately reflect the change.

The change register is to be updated to reflect the result of the change.

5.9 Pre-approved changes

Periodic, frequently repeated changes carried out in Information Systems can be classified as Pre-approved or Standard changes.

Pre-Approved changes must be initially documented on an RFC and presented to the CAB as a request to become a standard change.

Approval for such changes exists only as long as the RFC remains accurate, any deviations from that RFC will require a new RFC to be submitted for each differing change.

Reports on the implementation of pre-approved changes are to be submitted to the CAB post their implementation.

6 References

Document ID	Document Title
N/A	ISO 27005:2018 Information Security Risk management standard
N/A	ISO 31000:2018 Risk Management
N/A	ISO 9001:2015 Quality management system
N/A	NIST Responding to a Cyber Incident
N/A	Privacy Act 1988
N/A	Privacy Amendment (Notifiable Data Breaches) Act 2017

7 Related Documents

Document ID	Document Title
https://www.scee.com.au/privacy-policy	Privacy Statement
SCEE-BS-IT-POL-0005	Access Control Policy
SCEE-BS-IT-POL-0007	Backup and Recovery Policy
SCEE-BS-IT-POL-0011	Mobile Device Security & Remote Access Policy
SCEE-BS-IT-POL-0010	Patching & Vulnerability Management Policy
SCEE-BS-IT-POL-0008	Secure Disposal & Reuse Policy
SCEE-BS-IT-POL-0006	Supplier Relationship Policy
SCEE-BS-IT-POL-0004	Information Security Policy
SCEE-BS-IT-PLN-0001	Incident Management Plan
SCEE-BS-IT-TEM-0001	Network User Account Request Form
SCEE-BS-IT-TEM-0002	Deactivate Network User Request Form
SCEE-BS-IT-TEM-0003	JDE New Change User Request Form
SCEE-BS-IT-TEM-0005	Insight New Change User Request Form
SCEE-BS-PO-TEM-0021	Disposal Asset Approval
SCEE-BS-QU-MAN-0001	Quality Manual
SCEE-CI-AD-RSR-010	Operations RIR Dec 20Secure Disposal & Reuse Policy
SCEE-CM-CN-TEM-0025	Confidentiality Agreement – SCEE Disclosing Information
SCEE-CM-CN-TEM-0026	Confidentiality Agreement – Both Parties Disclosing Information
SCEE-CM-CN-TEM-0027	Confidentiality Agreement – Risk Checklist
SCEE-MN-CG-PLN-0001	Business Continuity Plan
SCEE-MN-CG-POL-0007	Code of Conduct

Appendix A Change Request Form (RFC)

This form is available digitally through scee.data-track.com.au.

Change Request Form				
Change Number:	*[**Delete before use**: As recorded within the change register]*			
Name of Information system (application, infrastructure etc.)				
Requestors Name/Role Title				
Business Unit Manager	*[Enter the name of the business unit manager responsible for the system]*			
Brief Description of Change Request				
Pre-approved Change?	**Yes/No**			
Schedule and period of outage	*[**Delete before use:** For Pre-approved changes specify schedule and outage requirements]*			
Date Submitted				
Requested change date				
Priority (please clearly state if this is an emergency change)	☐ Low	☐ Medium	☐ High	☐ Critical
Reason for Change				
Approval by Business Unit Manager	**Name**		**Sign**	
To be completed by Information Technology Team				
Impact Analysis				
Resources required including costing				
Implementation Plan				
Outage, if any	*[**Delete before use**: - Server re-boot is considered to be an outage]*			
User Training required?	**Yes/No**			
Roll back Plan				

Impacted Information assets and owners			
Impacted business functions			
Conditions required by CAB			
Approval Signature(s) – CAB Chair		**Date Signed**	