SECURE
CYBER
GATES

CHANGE MANAGEMENT POLICY

SECURE
CYBER
GATES

DOCUMENT CONTROL PAGE

Document ID	SCG/CMP/028/1.0
Security Classification	Confidential
Date Issued	23-June-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	23-June-2025		Issued for internal review
1.0	23-June-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	23-June-2025		Issued for internal review
1.0	23-June-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	23-June-2025		Issued for internal review
1.0	23-June-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
23-June-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/RXT/037/1.0			Risk Exception Template

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

1) Objective 6

3) Scope 7

4) Configuration Change Control 7

4.1) Control Objective 7

4.2) Guidelines 7

5) Change Management 8

5.1) Control Objective 8

5.2) Change Management Process 8

5.3) Change Request Deployment process 10

5.4) Emergency Change Request 10

6) Employee Training and Awareness 10

7) Compliance and Monitoring 11

8) Escalation Matrix 11

9) Policy Exceptions 11

10) Policy Review and Updates 12

11) Conclusion 12

1) Objective

Our Change Management Policy serves as guidance for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise.

This Change Management Policy establishes the standards that promote fairness in ensuring all technology changes to production environments follow a standard process to reduce the risk associated with change. [SecureCyberGates] requires active stakeholder involvement to ensure changes are appropriately tested, validated, and documented before implementing any change on a production network.

This Policy applies to anyone who conducts business for or on behalf of [SecureCyberGates] including:

- All employees
- Management and company owners
- External business partners who act on [SecureCyberGates]'s behalf or in our interest as Third Party Representatives

It is important to note that every situation may not be addressed in this Change Management Policy; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from the Security, IT or Support team. Each and every one of us are responsible for ensuring that we follow these guidelines, and we will be held accountable for upholding our commitments to this Change Management Policy.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Accountable - Overseeing the implementation and enforcement of this policy [Review and Approve Policy]
DPO [Data Privacy Officer]	Responsible to review this Policy.
IT/ Security Team / Project Team	1. Responsible for ensuring Change management requirements are in place. 2. Responsible for enforcing these requirements. 3. Overseeing the implementation and enforcement of this policy.
BU Heads or Project	1. Ensuring that employees under their supervision comply with this policy. [Review and Approve this Policy].

Managers	
Employees / Contractors	1. Ask questions /Provide Feedbacks 2. Report possible or actual violations of this Policy. 3. Understanding and complying with this policy and related procedures.

3) Scope

This policy applies to all [SecureCyberGates] employees, contractors, and third-party representatives involved in initiating, planning, implementing, or managing changes to [SecureCyberGates] 's and Clients IT environment, including but not limited to:

- Hardware and software systems
- Applications and databases
- Network infrastructure
- Cloud and on-premises environments

4) Configuration Change Control

4.1) Control Objective

The organization follows change control processes and procedures for all changes to system components. The organization

- Determines the types of changes to systems that are configuration controlled.
- Approves configuration-controlled changes to systems with explicit consideration for security impact analysis.
- Documents approved configuration-controlled changes to systems.
- Retains and reviews records of configuration-controlled changes to systems.
- Audits activities associated with configuration-controlled changes to systems; and
- Coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board) that convenes on a routine basis.
- Updating the inventory as necessary.

4.2) Guidelines

Configuration change controls for organizational systems involve the systematic proposal, justification,implementation, testing, review, and disposition of changes to the systems, including system upgradesand modifications.

Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, databases , applications, firewalls, routers, and mobile devices), unscheduled / unauthorized changes and changes to remediate vulnerabilities.

5) Change Management

5.1) Control Objective

All changes to the IT environment for [SecureCyberGates] and Clients, whether routine, major, or emergency, must adhere to the following Standard. Changes must be submitted, reviewed, approved, and communicated as per the processes defined herein.

5.2) Change Management Process

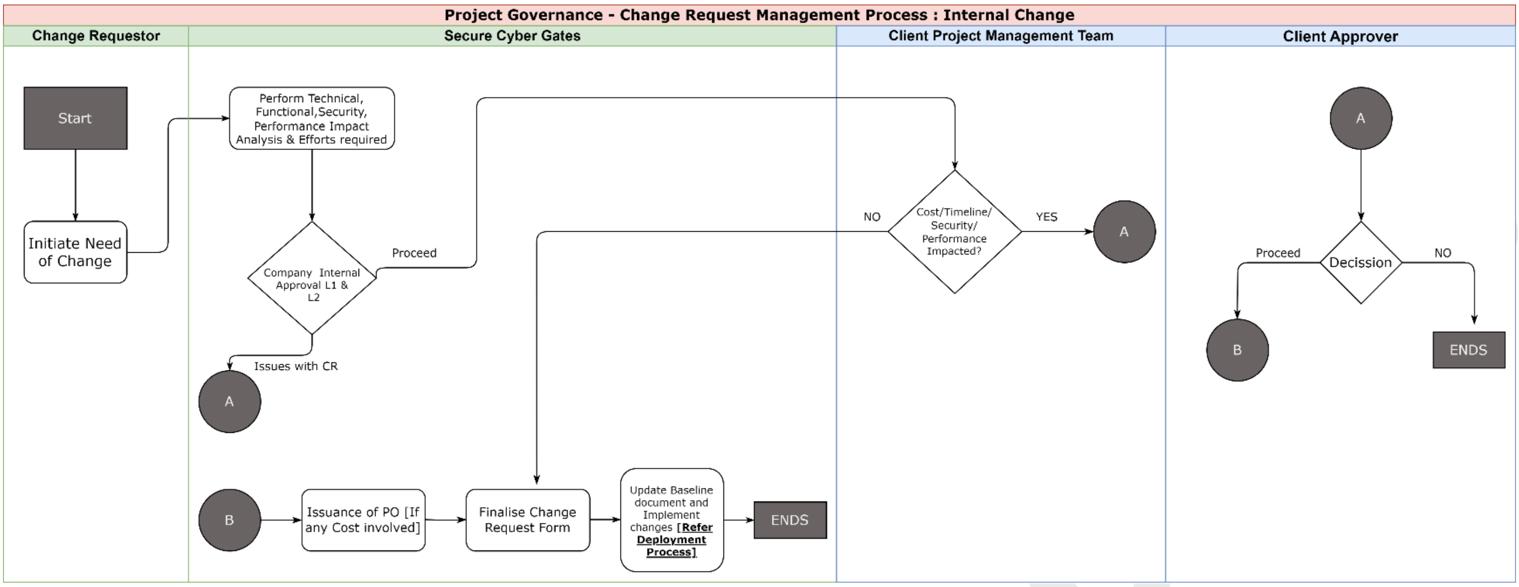
Changes in any form during the lifetime of the project will be handled via the Change Control Process. Controlling change to scope, requirements, and deliverables requires the support and participation of the entire Project Team. There will be a scope freeze upon Functional Specification Document (FSD) sign off. Any changes after the Functional Specification Document sign off will be considered as a change request which will have to go through the change control process.

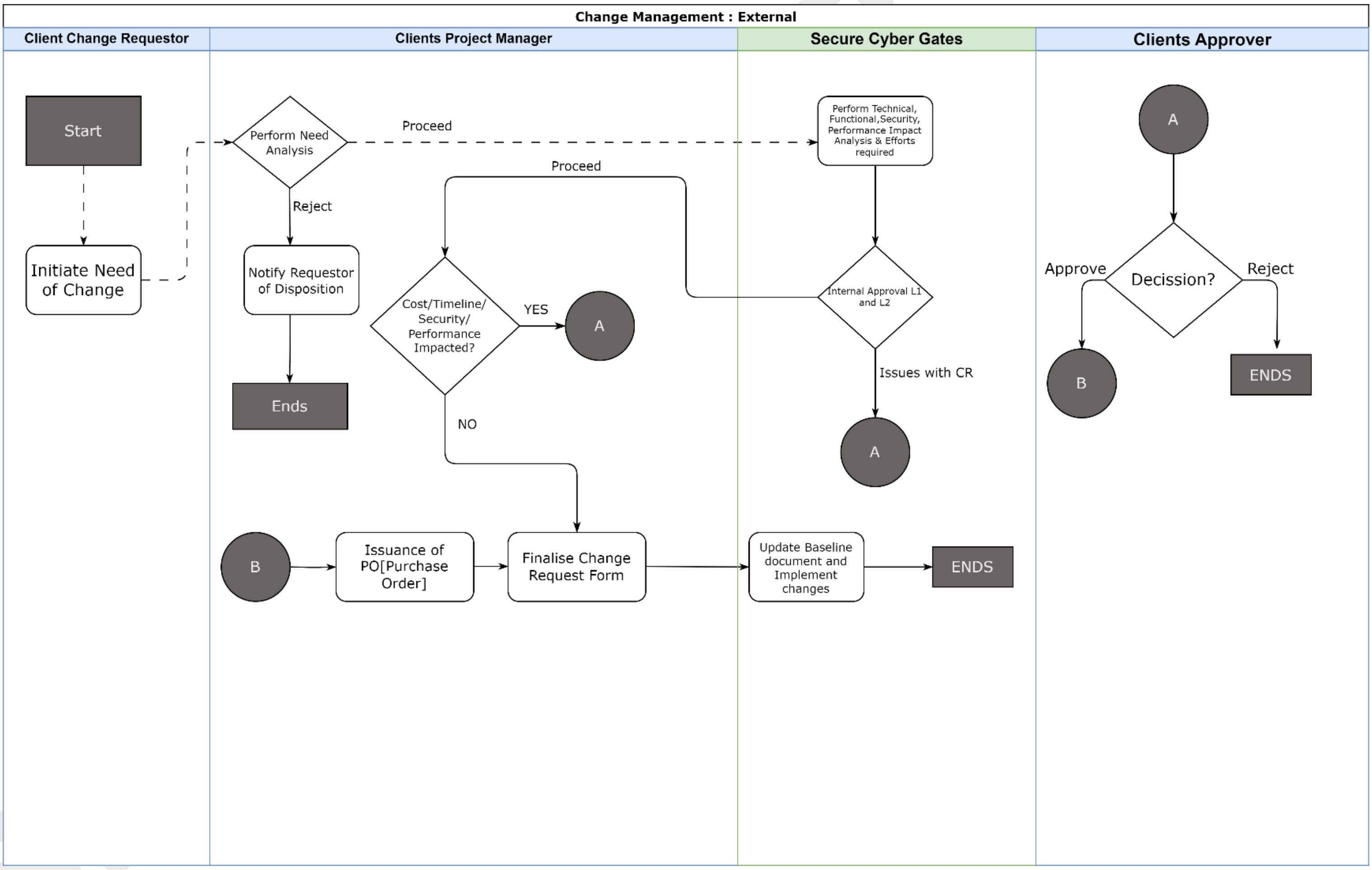
To manage project scope, we will manage change requests using a change control process. The change control process will require any change requests to be logged using a standard **Change Request Form [Document ID : SCG/CGRF/031/1.0]** which will have to be submitted to the project management team. The Project Management team, which consists of both project managers from [SecureCyberGates] and Customer is responsible for considering the impact of any user change request on the scope of the project.

Submitted change requests will be maintained in the **Change Request Log**. Any modification or deviation from the Functional Specification Document sign off or standard functionality or extension of project timeline, or changes to the time or costs will have to be reviewed by the Project Management team. [SecureCyberGates] or Customer may initiate the Change Request process whenever there is a perceived need for a change that will affect the overall costs, timeline or functionality, Security or Performance of the project. [SecureCyberGates] would perform Technical, Functional, Security and Performance Analysis for the new CR, if there are any risks then it will highlight it to Clients PM for the next decision.

The Client PM team will then need to escalate the change requests, their evaluation and recommendation to the [SecureCyberGates]'s Project Manager and the Customer Project Director. The scope of changes resulting in a requirement for additional project funding may require additional levels of approvals from [SecureCyberGates] or Customer. The impact on schedule and effort due to this scope change will be incorporated in the project plan

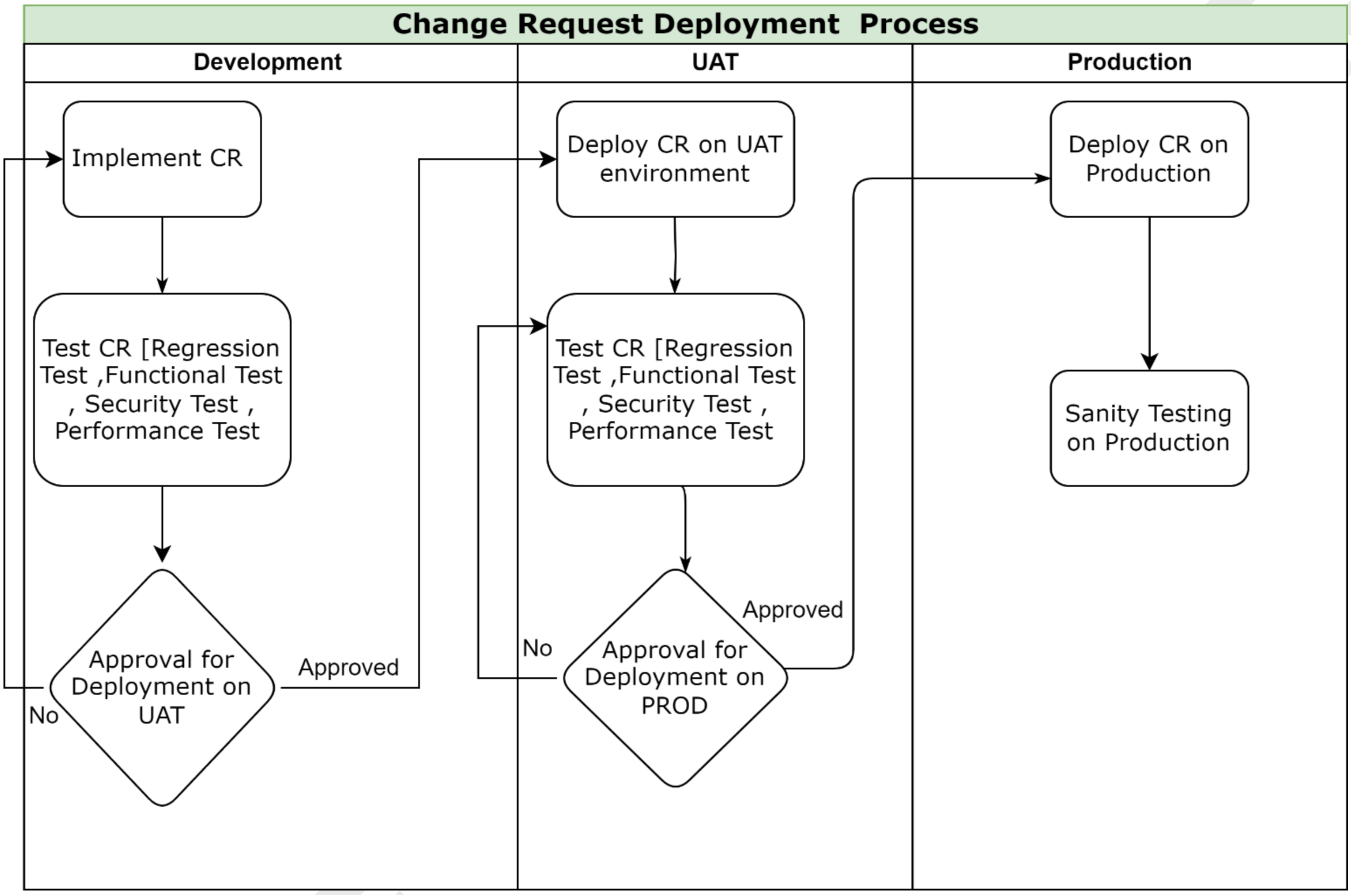
For any change request coming from [SecureCyberGates] internal staff, after need analysis is approved, Technical, Functional, Security and Performance analysis would be carried out and all risks would be reported to the concerned team. After internal approval [SecureCyberGates] team would communicate this to Client PM and once received an approval, [SecureCyberGates] team would proceed with implementing and deploying this CR.


Project Governance - Change Request Management Process : Internal Change
Change Requestor
Secure Cyber Gates
Client Project Management Team
Client Approver
Start
Initiate Need of Change
Perform Technical, Functional,Security, Performance Impact Analysis & Efforts required
Company Internal Approval L1 & L2
Proceed
Issues with CR
A
Cost/Timeline/ Security/ Performance Impacted?
NO
YES
A
A
Decission
Proceed
NO
B
ENDS
B
Issuance of PO [If any Cost involved]
Finalise Change Request Form
Update Baseline document and Implement changes [Refer Deployment Process]
ENDS


Change Management : External
Client Change Requestor
Clients Project Manager
Secure Cyber Gates
Clients Approver
Start
Initiate Need of Change
Perform Need Analysis
Proceed
Reject
Notify Requestor of Disposition
Ends
Perform Technical, Functional,Security, Performance Impact Analysis & Efforts required
Proceed
Internal Approval L1 and L2
Issues with CR
A
Cost/Timeline/ Security/ Performance Impacted?
YES
A
NO
A
Approve
Decission?
Reject
B
ENDS
B
Issuance of PO[Purchase Order]
Finalise Change Request Form
Update Baseline document and Implement changes
ENDS

5.3) Change Request Deployment process

Approved CR would be implemented and tested, after approval this CR would be deployed to UAT. Testing would be performed on UAT and after approval from both [SecureCyberGates] PM and Client PM, changes would be deployed to Production. A quick sanity testing may be carried out on production to ensure basic functionalities are working.


Change Request Deployment Process
Development
UAT
Production
Implement CR
Test CR [Regression Test ,Functional Test , Security Test , Performance Test
Approval for Deployment on UAT
No
Approved
Deploy CR on UAT environment
Test CR [Regression Test ,Functional Test , Security Test , Performance Test
No
Approved
Approval for Deployment on PROD
Deploy CR on Production
Sanity Testing on Production

5.4) Emergency Change Request

For any Emergency Change, after a quick approval from Client PM and [SecureCyberGates] , it would be implemented and tested on Development environment then to UAT and then to Production. For Emergency CR , team may skip implementation on Development and directly implement on UAT if the changes are minor and then push to Production.

6) Employee Training and Awareness

6.1) All [SecureCyberGates] employees SHOULD undergo training and assessment on this policy during their initial induction [Onboarding].

6.2) Security team to conduct periodic trainings **ATLEAST ONCE** a year.

7) Compliance and Monitoring

7.1) Compliance with this policy is **MANDATORY**. Employees violating this policy will be subject to disciplinary action up to and including termination.

7.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may have their access to [SecureCyberGates]systems , Application and networks revoked or suspended until compliance is achieved. Repeated or severe violations may result in the termination of their contracts or business relationships with [SecureCyberGates].

7.3) Periodic Audits and Assessments : [SecureCyberGates]'s IT department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this security policy.

8) Escalation Matrix

8.1) In case of any policy violations issues, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Level	Role	Contact
Level 1	Team Lead /Reporting Manager	First-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 2	Group Manager / Senior Managers	Second-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 3	CISO	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

8.2) Employee SHOULD provide sufficient evidences and details , Clear description of the issue.

8.3) Security team to define issue severity and proper SLA for issue resolution as per severity.

9) Policy Exceptions

9.1) There may be requirements where Employee needs policy exception for legitimate reasons, In such cases, employee should follow POLICY EXCEPTIONS template and approval process. **[Kindly refer Policy exception form [Document ID SCG/PXF/008/1.0]]**

10) Policy Review and Updates

10.1) This policy shall be periodically reviewed **[Atleast Once in a YEAR]**and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives,legal requirements and industry best practices.

10.2) Feedback from employees, stakeholders, and external audits shall be solicited and considered for continuous improvement of the policy and associated procedures.

10.3) Regular audits and inspections shall be conducted to assess compliance with this policy and associated procedures, with non-conformances addressed through corrective actions and preventive measures.

10.4) Any updates or revisions to this policy will be communicated to all employees and relevant stakeholders through appropriate channels. Employees are responsible for familiarizing themselves with the latest version of the policy and adhering to its requirements.

11) Conclusion

[SecureCyberGates] is committed to protecting the confidentiality, integrity, and availability of its data and information assets through the implementation of appropriate security controls. By adhering to the requirements and guidelines outlined in this policy, [SecureCyberGates] aims to minimize the risk of unauthorized access, data breaches, and other security incidents, while ensuring compliance with applicable laws, regulations, and industry standards, including the SOC 2 standard.

THANKYOU!

FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://securecybergates.com/services
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com