SECURE CYBER GATES

DOCUMENT CONTROL POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/DOCCP/006/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-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

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

The objective of this policy is to establish a robust framework for the control, management, and maintenance of **documents and records** throughout [SecureCyberGates] to ensure accuracy, integrity, accessibility, and compliance with relevant standards and regulations.

2) Scope

This policy applies to all **documents and records** generated, received, maintained, or used by employees, contractors, consultants, and any other personnel acting on behalf of [SecureCyberGates]. It encompasses both electronic and hardcopy formats and encompasses all aspects of document control, including creation, review, approval, distribution, access, storage, retrieval, revision, retention, disposal, and continuous improvement.

3) Responsibilities

Roles	**Responsibilities**
CISO	Overseeing the implementation and enforcement of this policy
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy.
Employees / Contractors	Adhering to this policy and following the prescribed procedures for document control.

4)Document and Record Creation

4.1) All documents and records shall be created using approved software and templates, where available, to ensure consistency and compatibility.

4.2) To create any new document / record , All Employees / Contractors **MUST** follow “Base Template Instructions” Document [ID : SCG/BASEINS/005/1.0] [NAME : SCG_BASE-DOCUMENT-INSTRUCTIONS_005_V1.0]

4.3) Each document or record shall be assigned a unique identifier [Document ID], version number, effective date, and author for traceability and accountability.

4.4) Documents and records shall adhere to a standardized format, including sections for purpose, scope, references, definitions, and any other relevant information as per standard templates.

5) Review and Approval

5.1) All new documents and revisions shall undergo a formal review and approval process conducted by designated reviewers and approvers.

5.2) Final approval shall be obtained from the appropriate authority before the document or record is released for use.

5.3) Documentation of review and approval activities shall be maintained for audit trail purposes. [e.g. Employee creates a new Document and ask for review and approval on email , Respective parties should review and approve over email and Sign the document , This Email should be attached inside the newly created document for Tracking/Audit purpose. Alternatively if any tool like JIRA/Clickup are used for review and approval then proper screensot from the tool should be attached inside the newly created document]

6) Distribution and Access Control

6.1) Approved documents and records shall be distributed electronically to authorized personnel through secure channels, such as email, document management systems, or collaboration platforms.

6.2) Distribution list section should be provided under “DOCUMENT CONTROL PAGE” section for every document / record. This states that document can be shared ONLY with the members included under Distribution list. Employee / Contractor MUST NOT share this document outside Distribution list.

6.3) Access to sensitive or confidential documents and records shall be restricted based on the principle of least privilege, with access permissions regularly reviewed and updated as necessary.

6.4) Employees shall receive training on document handling and security best practices to ensure proper handling and protection of sensitive information. This training SHOULD be repeated **atleast 1 time** every 6 months for all Employees/Contractors.

7) Storage and Retrieval

7.1) Documents and records shall be stored securely in designated electronic repositories or physical locations, depending on their format and sensitivity.

7.2) Documents and records shall be organized logically within repositories to facilitate easy retrieval and navigation, with appropriate indexing and categorization.

7.3) Backup and disaster recovery measures shall be implemented to safeguard against data loss or corruption.

8) Revision and Change Control

8.1) A formal **change control process** shall be established to manage revisions and updates to documents and records, including the documentation of changes and the maintenance of revision history.

8.2) Obsolete versions of documents and records shall be archived or removed from circulation to prevent unintended use and ensure users access the latest version.

9) Retention and Disposal

9.1) Retention periods for documents and records shall be established based on legal, regulatory, operational, and business requirements, with clear guidelines for retention and disposal.

9.2) Documents and records shall be disposed of securely at the end of their retention period through methods such as shredding, secure deletion, or other approved means.

10) Continuous Improvement

10.1) This document control policy shall be periodically reviewed and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives 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.

11) Training and Awareness

11.1) All employees shall receive training on this document control policy, including their roles and responsibilities in document management and compliance.

11.2) Ongoing awareness campaigns and refresher training shall be conducted to reinforce the importance of document control and promote a culture of compliance within [SecureCyberGates].

12) Monitoring and Auditing

12.1) 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.

12.2) Audit findings and corrective actions shall be documented and monitored to ensure effective resolution and continual improvement of document control practices.

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://www.youtube.com/@SECURECYBERGATES
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com