DATA RETENTION POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/DRTP/021/1.0
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
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

2) Roles &Responsibilities 6

3) Scope 6

4) Data Retention 6

5) Data Shredding Procedure 7

6) Employee Training and Awareness 8

7) Compliance and Monitoring 8

8) Escalation Matrix 8

9) Policy Exceptions 9

10) Policy Review and Updates 9

11) Conclusion 10

1) Objective

The objective of this document is to govern Data retention, and security of the Company's data as required by the Company's interests, contractual requirements, and as mandated by applicable laws and regulations. It is expected from all employees who are engaged with or on behalf of [SecureCyberGates], to understand and follow the below. Failure to do so can put future participation at risk. This policy will evolve as new technologies emerge.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Accountable - Overseeing the implementation and enforcement of this policy [Review and Approve Policy]
DPO [Data Privacy Officer]	Responsible for creating ,updating, and maintaining this policy.
IT/Security Team	1. Responsible for ensuring Data classification protection requirements are in place 2. Responsible for enforcing these Data classification requirements
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review and Approve this Policy]
Employees / Contractors	1. Read this this Policy 2. Ask questions /Provide Feedbacks 3. Report possible or actual violations of this Policy.

3) Scope

The policy contained herein applies to any person who has access to [SecureCyberGates]'s data and/or uses any of the [SecureCyberGates]'s Information resources/ assets. The purpose of this document is to elicit the best practices for data retention associated with [SecureCyberGates] and sets the framework required to ensure uniformity in participation.

4) Data Retention

Data retention provides a systematic review of the retention of data as part of its business process. The policy identifies data that should be maintained in an archive. The objective of this policy is to establish an effective control mechanism for the retention of data generated during the course of the business.

[SecureCyberGates] shall retain the data related to specific clients for the period defined by **the client for different project needs[Aligning with Regulatory Laws]**. When the retention period of the data expires, with due consent from the concerned client, [SecureCyberGates] shall erase or destroy the data in a manner adequate with its

technology and as agreed with the data owner
Our solution by default keeps **data online for 2 years** and in archival for **5 additional years.** Logs are maintained for **3 months**. Changes may be made to this retention period at request from the customer. Data that is no longer required will be securely disposed of.

Data Type	Description	Retention Time
Application/System Logs	Details of Logs maintained for all Products and Systems	1 YEAR
Database Archives	Once Customer Data is Deleted [e.g. Customer has deleted Some records from Some application [SOFT DELETE from DB and goes to DB Archives and then HARD DELETE after 1 YEAR]	1 YEAR
Employee Records	Regulatory Laws [Keep Employee Records after Employees Leaves Company]	10 YEARS
Company Financial Records	For TAX Audits	10 YEARS
CCTV Footage	CCTV footage for Sensitive areas	90 Days
EMAILS	All Email Communications	5 YEARS
SIEM Logs	Security Information and Event Management Logs for Forensic and incident investigation	5 YEARS
Project Documents	All Customer Contracts and Project Papers [Post Contract Terminations]	10 YEARS

NOTE: Actual Retention time depends on Project Contract and Regulatory Laws.

5) Data Shredding Procedure

The IT Team, Security and legal compliance teams periodically verify the asset inventory to document latest updates, process for recertification's or upgrades or renewal of subscriptions where necessary. This procedure ensures validity of both physical assets & intellectual property over time.
1) Identification of customers whose data needs to be shredded Support team identifies the client whose data needs to be shredded after getting data from Management.
2) Creation of data shredding ticket Support creates a "ServiceNow" ticket mentioning the name of the client whose data needs to be shredded and assigns it to IT team looping Security and management.
3) Scripts to shred the data
   a. Shredding script is run against a client of which the data needs to be removed. The scripts are run to clean the data for both master data and analytics/Log data.

b. The DB instance in other environments, which are created using the production DB, is refreshed after shredding so that the client data is removed from all environments.
c. The automated backup files roll back in **35 days** so that all the data in backups is also removed. A calendar event is created to track the same
d. After 35 days all the manual snapshots which are older than 35 days are also physically deleted.
e. Till the process is complete the “ServiceNow” ticket remains in In-Progress state
f. After 35 days, the “ServiceNow” ticket is marked for review and sent back to the Support team.
g. Support team intimates the client about the data being shredded and marks the ticket done.

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	First-level escalation: Email / Any Ticketing Tool

	Manager	[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

By implementing and adhering to this comprehensive Incident Management policy, [SecureCyberGates]aims to resolve incident ASAP and protect its sensitive information, intellectual property, and critical systems from unauthorized access and data breaches. This policy aligns with industry best practices and incorporates robust requirements for password construction, protection, management, and system development standards.

SECURE CYBER GATES

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

SECURE CYBER GATES