SECURE CYBER GATES

PRIVACY POLICY

SECURE CYBER GATES

DOCUMENT CONTROL PAGE

Document ID	SCG/PP/017/1.0
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/S2RAS/113/1.0			SOC2 Asset Scope
SCG/VL/033/1.0			List of Vendors

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

At [SecureCyberGates] , the protection of Personally Identifiable Information (PII) is a top priority. This policy outlines the steps that must be taken to ensure that PII is collected, processed, and stored securely and in accordance with industry standards and regulatory requirements [Malaysian PDPA Personal Data Protection Act 2010].

This Policy applies to anyone employed by or conducting business for [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 this Privacy Policy may not cover every possible scenario. If you are unsure how the standards or guidelines apply in a given situation, please seek guidance from the HR Manager or relevant department heads.
Each individual is responsible for ensuring compliance with these guidelines, and all stakeholders will be held accountable for upholding their commitments to this Privacy Policy.

2) Roles &Responsibilities

Roles	Responsibilities
CISO / Security Team	Review and Audit this Policy.
HR Team	Overseeing the implementation and enforcement of this policy.Create, Manage, Monitor, Maintain, Audit this Policy.
BU Heads or Project Managers	Ensuring that Employees/Contractors/Vendors under their supervision comply with this policy. [Review this Policy]
Employees / Contractors / Vendors	1. Read this Policy 2. Ask questions / Provide Feedbacks 3. Report possible or actual violations of this Policy.

3) Scope

This policy applies to all departments, employees, contractors, and third-party service providers of [SecureCyberGates]. It covers all forms of PII, including but not limited to names, addresses, Social Security numbers [MyKad], driver's license numbers, passport numbers, financial information, and biometric data.

4) Collection of PII

PII shall only be collected for legitimate business purposes and with the consent of the individual to whom the information belongs. The following steps shall be taken to ensure the secure collection of PII:

Purpose: The purpose for collecting PII shall be clearly stated, and the information shall only be used for the stated purpose.

Consent: Consent shall be obtained from the individual to whom the information belongs before PII is collected.

Minimization: PII shall be collected only to the extent that is necessary for the stated purpose.

Security: Appropriate security measures shall be implemented to protect the PII during collection, such as encryption and secure storage.

Notice: Individuals shall be notified about the PII being collected, the purpose for collection, and the intended use of the information.

5) Processing of PII

The following steps shall be taken to ensure the secure processing of PII:

Access Control: Access to PII shall be controlled by implementing authentication and authorization mechanisms, such as user IDs and passwords, and managing access privileges.

Confidentiality: PII shall be kept confidential and not disclosed to unauthorized parties.

Accuracy: PII shall be accurate, complete, and up-to-date, and shall be corrected if necessary.

Retention: PII shall be retained only for as long as necessary for the stated purpose and shall be disposed of securely when no longer needed.

Integrity: Measures shall be implemented to ensure the integrity of PII during processing, such as checksums and digital signatures.

6) Storage of PII

The following steps shall be taken to ensure the secure storage of PII:

Encryption: PII shall be encrypted while stored, both at rest and in transit.

Access Control: Access to stored PII shall be controlled by implementing authentication and authorization mechanisms, such as user IDs and passwords, and managing access privileges.

Backup: Regular backups shall be taken of stored PII, and these backups shall be stored in a secure location.

Physical Security: Physical access to stored PII shall be controlled by implementing appropriate security measures, such as locks, access control systems, and video surveillance.

Logging and Monitoring: Logging and monitoring mechanisms shall be implemented to detect and respond to potential security incidents involving stored PII.

7) Incident Management

In the event of a security incident involving PII, [SecureCyberGates] shall respond in a timely and effective manner. The following steps shall be taken:

Report the incident: The incident shall be reported to the appropriate department or individual, such as the information security officer or the incident response team.

Investigate the incident: The incident shall be investigated to determine the cause, the extent of the breach, and the information that has been disclosed.

Notify affected individuals: Affected individuals shall be notified in accordance with applicable laws and regulations.

Implement remedial actions: Remedial actions shall be implemented to prevent the recurrence of similar incidents and to restore the confidentiality, integrity, and availability of the information.

Incident Response Plan: A comprehensive incident response plan shall be developed and regularly updated to ensure effective and coordinated response to PII-related security incidents.

8) PII Protection

Data Protection by Design and Default

[SecureCyberGates] shall adopt a "data protection by design and default" approach, ensuring that PII protection measures are integrated into the design and development of all systems, products, and services that handle PII.

Privacy Impact Assessments

Privacy Impact Assessments (PIAs) shall be conducted for all new projects, systems, or processes that involve the collection, processing, or storage of PII, to identify and mitigate potential privacy risks.

Third-Party Service Providers

Third-party service providers who handle PII on behalf of [SecureCyberGates] shall be required to comply with this policy and implement appropriate security measures to protect PII. A vendor management program **[Refer Document ID: SCG/VMP/016/1.0]** shall be established to ensure that third-party service providers who handle PII on behalf of [SecureCyberGates]are regularly assessed and monitored for their compliance with PII protection requirements.

9) Employee Training and Awareness

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

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

10) Compliance and Monitoring

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

10.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may have their access to [SecureCyberGates]systems 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].

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

11) Escalation Matrix

11.1) 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	HR	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

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

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

12) Policy Exceptions

12.1) 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]]**

13) Policy Review and Updates

13.1) 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.

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

13.3) 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.

13.4) 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.

14) Conclusion

[SecureCyberGates]is committed to maintaining the highest standards for PII Protection. Every Vendor/ Employee plays a crucial role in safeguarding confidential information, and their diligence and cooperation are essential for the successful implementation of this policy.

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

SECURE CYBER GATES