INFORMATION SECURITY POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/INFSP/030/1.0
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

SECURE CYBER GATES

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

SECURE CYBER GATES

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.

SECURE CYBER GATES

Contents

SECURE CYBER GATES

SECURE CYBER GATES

1) Objective

This Information Security Policy defines the policies and procedures for preserving the confidentiality, integrity, and availability of [SecureCyberGates]'s information assets. Information security refers to the processes and methodologies designed and implemented to protect all forms of information and data controlled by [SecureCyberGates]'s from unauthorized access, use, disclosure, disruption, modification, or destruction.

The objectives of this policy are:

- Ensure [SecureCyberGates]'s information resources are appropriately protected
- Provide a consistent set of security standards across [SecureCyberGates]'s
- Reduce vulnerabilities and security risks to an acceptable level
- Support [SecureCyberGates]'s business operations and compliance requirements

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	1. Responsible for ensuring Information security requirements are in place. 2. Responsible for enforcing these requirements. 3. Overseeing the implementation and enforcement of this policy.
BU Heads or Project Managers	1. Ensuring that employees under their supervision comply with this policy. [Review and Approve this Policy].
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 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

4) Policy Principles

[SecureCyberGates]'s information security principles are based on industry best practices and compliance requirements, including:

- ISO/IEC 27001 Information Security Management Standards
- SOC2
- Malaysia Personal Data Protection Act 2010 (PDPA)
- Bank Negara Malaysia Risk Management in Technology (RMiT)
- PCI-DSS

The core principles are:

Confidentiality

Protecting information from unauthorized disclosure or access. The "need-to-know" principle is employed.

Integrity

Maintaining the accuracy, completeness, and consistency of information over its lifecycle. Preventing unauthorized modification.

Availability

Ensuring information and services are accessible and usable when needed by authorized users/systems.

5) Governance and Organization

5.1) Roles and Responsibilities

The organization regularly updates recovery strategies to keep current with business needs and technology changes.

Information Security Steering Committee:

- Provides executive oversight and approves security policies/standards
- Includes CEO, CTO, CINO, Information Security Officer, IT Manager and other executives

The committee is responsible for:

- Establishing management commitment and strategic direction for information security
- Approving security policies, standards and the security program
- Reviewing and providing oversight of security risks and issues
- Allocating appropriate resources for information security requirements

SECURE CYBER GATES

Information Security Officer (ISO):

- Develops, implements and maintains the Information Security Program
- Leads information security risk management activities
- Provides security training and awareness programs
- Investigates and manages security incidents

Information Owners:

- Ensure proper security controls for their information assets
- Define access requirements and data classification

IT and Information Security Teams:

- Implement and maintain technical security controls
- Monitor for security events and vulnerabilities
- Perform security testing and reviews

Managers and Leads:

- Ensure compliance with policies in their areas
- Address security violations by employees

All Employees and Third Parties:

- Complete security awareness training
- Follow all security policies and procedures
- Report suspected security incidents promptly

6) Human Resources Security

6.1) Prior to Employment

[SecureCyberGates] ensures the trustworthiness and suitability of new employees and contractors through background verification checks and confidentiality agreements, which cover:

- Education, qualifications and experience
- Criminal records checks (where permitted)
- References and recommendations
- CTOS check for applicable candidates.
- Contractual obligations for protecting confidential information

SECURE CYBER GATES

6.2) During Employment

All employees and contractors must complete the following security awareness and training activities:

- Information Security Awareness Training (upon hire and while there is an update)
- Secure Coding Practices

The training covers key security topics such as:

- Information handling and classification
- Secure use of IT systems and data
- Physical security controls
- Social engineering risks
- Incident reporting procedures

6.3) Termination and Changes

The procedures below where applicable have to be completed by every employee prior to their last day of employment at [SecureCyberGates].

I. Deletion of listed items from personal devices
   a. Company software
   b. Virtual Machines used for development, testing, training or other use
   c. Company documentation
   d. Company source code
   e. Company related correspondence, including email, proposals, pricing
II. Remove Email Access/Internal Apps from mobile device
III. Return of company notebook, notebook bag and notebook charger
IV. Return of access card
V. Return of business card
VI. Return of medical insurance card
VII. Return of parking card
VIII. Return of office keys
IX. Return of company documentation, books, DVDs e.t.c

The full exit checklist is verified by the employee's DRM or by a member from HR.

For more details please refer
HR Policy, DOC ID: SCG/HRP/012/1.0
Acceptable Usage Policy DOC ID: SCG/AUP/013/1.0
Code of Conduct Policy DOC ID: SCG/COC/014/1.0
Privacy Policy DOC ID: SCG/PP/017/1.0
Confidentiality Policy DOC ID: SCG/CNFP/018/1.0

SECURE CYBER GATES

7) Asset Management

7.1) Information Classification and Handling

[SecureCyberGates] employs a **Four-tier** classification system for labelling and handling different types of information:

Highly Confidential: Highly Confidential data like Production access details, Company Financial records , Payment details

Confidential: Sensitive data like trade secrets, intellectual property, unpublished financial records. Must only be accessed and shared on a strict need-to-know basis using secure methods. Examples: Source code, encrypted customer data.

Internal Use Only: Operational business data intended only for approved internal users at [SecureCyberGates] , Not for public disclosure. Examples: Employee records, sales reports, technical documentation.

Public: Information approved for public disclosure like marketing materials and press releases.

For more details please refer **Data Classification Policy, DOC ID: SCG/DCP/020/1.0**

7.2) Asset Inventory and Management

[SecureCyberGates] maintains an inventory of its key information assets, classifying each as software, physical or information assets. The inventory identifies:

- Description and owner of the asset
- Value, sensitivity and criticality of the asset
- Location, backups and redundancies
- Security controls applied to protect the asset

This inventory is reviewed annually and used for risk assessments, access controls, handling requirements and security control planning.

For more details please refer **Asset Management Policy, DOC ID: SCG/ASMP/027/1.0**

7.3) Secure Disposal and Reuse

Information assets being disposed of or re-allocated must have their data and software erased or destroyed using approved sanitization methods. Specific security measures include:

- Using secure wipe utilities for sanitizing storage devices
- Physically destroying storage media that cannot be sanitized
- Validating successful erasure before reusing devices

- Prohibiting insecure transfers of information during reallocation

For more details please refer **Media Disposal Policy, DOC ID: SCG/MSADP/022/1.0 and Data Retention Policy DOC ID : SCG/DRTP/021/1.0**

8) Access Controls

8.1) Access Management

Access to [SecureCyberGates]'s networks, systems, applications and data is controlled based on the principles of least privilege and need-to-know. An access control system is employed to request, establish, issue, and modify user access privileges tied to specific roles and responsibilities.

Processes are defined for:

- Managing and approving access requests
- Enforcing segregation of duties and privilege constraints
- Reviewing and removing obsolete user accounts/access rights
- Managing system and application access control lists

8.2) User Access Controls

Secure logon procedures and technical controls manage user access across [SecureCyberGates]'s IT assets, including:

- Use of unique user IDs to enable individual accountability
- Password complexity, expiration and protection requirements
- Enabling multi-factor authentication for high-risk accesses
- Logging and monitoring of failed access attempts
- Session timeouts and restriction of concurrent sessions
- Disabling inactive accounts and privileged default accounts

For more details please refer **Password Policy, DOC ID: SCG/PP/009/1.0**

8.3) Remote Access

Remote access to [SecureCyberGates]'s internal networks, systems and applications is permitted only through a managed and secured remote access facility. The requirements include:

- Use of multi-factor authentication mechanisms
- Encryption of remote access communications

- Logging and monitoring of remote sessions
- Annual revalidation and approval of remote user accounts
- Prohibitions on transferring sensitive data to remote devices

For more details please refer **Access Management Policy, DOC ID: SCG/AMP/010/1.0**

9) Physical and Environmental Security

9.1) Physical Access Controls

Entry to [SecureCyberGates]'s facilities is restricted through an access control system requiring badge credentials. Additional physical security controls include:

- Secure perimeter protections (fences, locks, alarms, guards, etc.)
- Separating areas by threat-risk and restricting access
- Supervising and monitoring visitor access and movement
- Secure furniture and equipment cabling
- Secure disposal procedures for equipment and sensitive waste

9.2) Equipment Protection

IT equipment and supporting infrastructure are protected from power failures, environmental threats, unauthorized access and other risks through controls such as:

- Uninterruptible power supplies and generators
- Fire detection and suppression systems
- Heating, ventilation and air conditioning controls
- Secure cable routing and equipment racking
- Maintaining designated secure equipment rooms/Server rooms

9.3) Clear Desk and Clear Screen

[SecureCyberGates] enforces clear desk and clear screen practices to prevent unauthorized data exposure through:

- Securing unattended documents, media and devices
- Enabling password-protected screensavers and secure logouts
- Prohibiting viewing of sensitive information in public areas
- Securely storing documents and devices after business hours

For more details please refer **Physical Security Policy, DOC ID: SCG/PSP/007/1.0**

10) Cryptography

10.1) Encryption and Key Management

Cryptographic controls are employed for protecting the confidentiality and integrity of [SecureCyberGates] 's information in the following scenarios:

- Transmission of data over public or untrusted networks
- Protection of sensitive data at rest on storage devices
- Use of secure encrypted communication channels like TLS, IPSec
- Implementation of trusted key generation, distribution and storage

[SecureCyberGates] maintains standards for approved cryptographic algorithms, protocols and key management processes.

10.2) Digital Signatures

[SecureCyberGates] uses digital signature controls based on approved standards for non-repudiation, authentication and data integrity in applicable business processes like:

- Digitally signing and verifying software code and updates
- Authenticating and authorizing electronic transactions/contracts
- Signing and certifying digital identities and certificates

For more details please refer **Cryptographic/ Encryption Policy, DOC ID: SCG/ENCP/025/1.0**

11) Operations Security

11.1) Protection from Malware

Anti-malware controls are deployed at multiple layers with centralized monitoring and management, including:

- Endpoint anti-malware protection on all servers, workstations
- Network malware inspection at Internet gateways
- Sandboxing and detonation chambers for analyzing suspected malware
- Automated update management for anti-malware signatures

For more details please refer **Endpoint Security Policy, DOC ID: SCG/ENDP/026/1.0**

11.2) Backup Management

[SecureCyberGates]'s backup management process covers:

- Documented backup schedules and storage requirements
- Monitoring and alerts for failed backups
- Testing data recovery and restoration annually
- Secure offsite storage of backups for business continuity
- Encryption of confidential data backups

For more details please refer **Data Backup Policy, DOC ID: SCG/DABP/024/1.0**

11.3) Logging and Monitoring

Logging mechanisms capture security events across networks, servers, applications and user activities for monitoring and analysis. Standards cover:

- Types of logs to enable for each technology component
- Centralized log management and retention requirements
- Real-time monitoring, analysis and correlation of events
- Reporting process for suspicious activities and alerts

11.4) Change and Release Management

Changes to [SecureCyberGates]'s IT infrastructure, operating systems and applications follow these processes:

- Use of separate development, test and production environments
- Review and approval workflow for changes
- Risk assessment for emergency changes
- Secure change build and deployment mechanisms

For more details please refer **Change Management Policy, DOC ID: SCG/CMP/028/1.0**

12) Communications Security

12.1) Network Security

[SecureCyberGates] employs layered network security controls including:

- Firewalls with strict ruleset controlling traffic flows
- Intrusion detection and prevention systems
- Network segregation and access control lists
- Secure wireless management processes
- Monitoring of network traffic patterns for threats

SECURE CYBER GATES

12.2) Data Transmission Security

[SecureCyberGates] requires use of the following controls for securing electronic data transmission:

- Encryption of data in transit over untrusted networks
- Implementation of secure file transfer mechanisms
- Use of secure remote access and wireless communication protocols
- Content filtering and inspection for emails and web communications

12.3) Email and Web Security

[SecureCyberGates] employs technical controls to protect against threats targeting email, messaging and browsing, such as:

- Anti-spam and anti-phishing filters
- Blocking of unauthorized or high-risk attachments
- URL filtering and website blacklists/whitelists
- Malware detection and quarantine for emails and downloads
- Email disclaimers and banners

For more details please refer **Network Security Policy, DOC ID: SCG/NWSP/023/1.0**

13) System Acquisition, Development and Maintenance

13.1) Security Requirements

Security requirements are established and treated as part of the solution architecture during acquisition or development of new information systems supporting [SecureCyberGates] 's business processes.

These include:

- Information security policy and controls requirements
- Regulatory and third-party compliance mandates
- Conducting risk assessments and security reviews
- Specifying technical security and hardening standards
- Requirements for ongoing security testing and monitoring

13.2) Secure Development Lifecycle

A secure system development lifecycle (SDLC) methodology incorporating security best practices are followed, covering activities such as:

- Security training for development teams
- Threat modelling and architecture risk analysis
- Secure coding practices and code reviews
- Security testing (SAST, DAST, penetration tests)
- Environment hardening and baseline builds
- Secure change and release management

13.3) Outsourced Development

For systems or software developed by third parties or suppliers, [SecureCyberGates] establishes formal agreements covering:

- Defined security requirements and secure coding standards
- Right to review code, designs and test results
- Acceptance testing by [SecureCyberGates] 's security teams
- Non-disclosure and intellectual property provisions
- Service levels and adherence to [SecureCyberGates] 's security policies

14) Supplier Management

14.1) Supplier Security Policy

[SecureCyberGates] maintains and reviews security requirements and performance for all suppliers and third parties involved in the design, development, delivery, operations or support of [SecureCyberGates]'s products and services.

The Supplier Security Policy defines:

- Security requirements in contracts and agreements
- Minimum security levels and compliance certifications
- Rights for security assessments and audits
- Non-disclosure commitments and data handling requirements
- Restrictions on subcontractor or offshore involvement

14.2) Outsourced Development

For any cloud services or external hosting, [SecureCyberGates] requires:

- Comprehensive security certifications like ISO 27001, SOC 2
- Meeting defined security and privacy requirements
- Undergoing security assessments and continuous monitoring
- Requirements for secure coding, operations and encryption
- Rights to audit security practices and inspect facilities

- Contractual safeguards and commitments

For more details please refer **Vendor Management Policy, DOC ID: SCG/VMP/016/1.0**

15) Security Incident Management

15.1) Incident Response Plan

[SecureCyberGates] maintains and tests an Incident Response Plan defining processes for:

- Monitoring and detecting potential incidents
- Establishing an incident response team and facility
- Escalation, containment and recovery procedures
- Evidence preservation and forensic investigations
- Notifying internal teams, customers and authorities
- Post-incident reviews and improvement plans

15.2) Employee Incident Reporting

All employees, contractors and third parties must promptly report any suspected security incidents or policy violations through designated reporting channels to [SecureCyberGates] 's security teams.

Protection is provided against retaliation or consequences for any personnel reporting issues in good faith. Not reporting known incidents is grounds for disciplinary action.

15.3) Incident Logging and Tracking

Mechanisms are implemented for centralized tracking and documentation of all reported security incidents, including:

- Unique references and details of each incident
- Categories based on the type, severity and status
- Chronological logs of investigation and response activities
- Impact assessments and lessons learned
- Management reports on incident metrics and trends

For more details please refer **Incident Response Plan & Procedure, DOC ID: SCG/IMP/019/1.0**

16) Business Continuity and Disaster Recovery

16.1) Planning and Processes

To ensure ongoing compliance, [SecureCyberGates] maintains security policies and standards aligned to:

- Legal and regulatory mandates
- Security frameworks and best practices
- Security zones and control baselines in its environment
- Applicable certifications like ISO 27001, SOC 2, PCI-DSS etc.
- Industry-specific security requirements

16.2) Compliance Monitoring

Activities conducted by [SecureCyberGates]'s compliance and security teams include:

- Security control assessments and gap analysis
- Risk assessments and mitigation planning
- Vulnerability assessments and penetration testing
- Monitoring security metrics

For more details please refer **Business Continuity & Disaster Recovery Policy, DOC ID: SCG/BCDRP/029/1.0**

17) Security Monitoring and Testing

17.1) Technical Monitoring

[SecureCyberGates] employs monitoring solutions and processes to detect and respond to security events across its IT infrastructure, including:

- Security Information and Event Management (SIEM)
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Data Loss/Leakage Prevention (DLP) controls
- Network and host-based security monitoring
- Application activity monitoring and user behaviour analytics

17.2) Vulnerability Management

A vulnerability management program identifies, prioritizes, and remediates software vulnerabilities across [SecureCyberGates]'s assets through:

- Periodic vulnerability assessment scans
- Subscribing to vulnerability intelligence feeds
- Patch management processes and deployment
- Risk evaluation and mitigation planning
- Penetration testing by internal/external teams

17.3) Audits and Assessments

Internal and external audits are conducted periodically to assess [SecureCyberGates]'s

security control environment, including:

- Compliance audits against standards like ISO 27001, SOC 2
- Internal self-assessments and gap analyses
- External third-party audits and certifications
- Physical security assessments of facilities
- Social engineering tests and phishing exercises

For more details please refer **Vulnerability & Patch Management Policy, DOC ID: SCG/VPMP/011/1.0**

18) Security Awareness and Training

18.1) Security Awareness Program

An ongoing awareness program promotes a security-conscious culture through activities such as:

- Annual security awareness training for all staff
- Regular phishing simulation exercises
- Communication campaigns and newsletters
- Physical security awareness (e.g., tailgating)
- Policy compliance reminders and updates

18.2) Roles-based Security Training

Additional role-specific training covers areas like:

- Secure application development
- Database security and data protection
- System/network administration security
- Social engineering risks for client-facing roles
- Incident response and forensics procedures
- Risk Management Program

19) Security Awareness and Training

19.1) Risk Assessment Methodology

[SecureCyberGates] follows a risk-based approach to identify, assess and mitigate information security risks through:

- Asset valuation and impact assessment
- Threat identification and likelihood estimation
- Quantitative and qualitative risk analysis models

- Treatment through preventive/detective/corrective controls
- Formally accepting, transferring or avoiding residual risks

19.2) Continuous Improvement

Risk assessments are conducted periodically and integrated with processes like:

- New projects, systems or major changes
- Emerging threats or significant incidents
- Internal audits and security reviews
- External changes impacting the risk landscape
- Driving the security strategy and road-map

For more details please refer **Risk Management Policy, DOC ID: SCG/RMF/015/1.0**

20) Employee Training and Awareness

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

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

21) Compliance and Monitoring

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

21.2) 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].

21.3) 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.

22) Escalation Matrix

22.1) 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	Second-level escalation: Email / Any Ticketing Tool

	Managers	[info@securecybergates.com]
Level 3	CISO	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

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

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

23) Policy Exceptions

23.1) 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]]**

24) Policy Review and Updates

24.1) 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.

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

24.3) 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.

24.4) 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.

25) 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.

SECURE CYBER GATES

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

SECURE CYBER GATES