SECURE CYBER GATES

CONFIDENTIALITY POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/CNFP/018/1.0
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

During their tenure, employees may encounter Sensitive Information. All Sensitive Information, regardless of its form (spoken, written, or electronic), must be handled in a way that preserves its confidentiality. Unauthorized disclosure of such Sensitive Information may lead to adverse financial consequences, competitive disadvantages, reduced productivity, or legal ramifications for [SecureCyberGates].
Authorized personnel at [SecureCyberGates] are expected to handle Confidential Information with respect and diligence. Those granted access to such information are responsible for ensuring its confidentiality and limiting access as per permissions and legal requirements. Access to Confidential Information should align with the individual's job responsibilities. Any breach of this policy or regulatory requirements constitutes unauthorized or inappropriate use, disclosure, or access of Confidential Information.
[SecureCyberGates] recognizes the critical importance of maintaining the confidentiality of sensitive information, including but not limited to trade secrets, intellectual property, financial data, employee records, and customer information. Protecting confidential information is essential for maintaining the trust of our stakeholders, preserving our competitive advantage, and ensuring compliance with legal and regulatory requirements.

This policy outlines the principles and procedures for handling confidential information within [SecureCyberGates],It applies to all employees, contractors, consultants, and any other individuals or entities that may have access to [SecureCyberGates] 's confidential information. By adhering to this policy, we aim to create a secure and ethical environment that fosters trust and protects the company's interests.

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.

More details on roles and responsibilities are outlined below:

Employees / Contractors / Vendors:

Handling Confidential Information Securely:

- Employees must follow strict protocols when accessing, transmitting, or storing confidential data.
- Encryption, access controls, and secure channels are essential.

Prompt Reporting of Breaches:

- Any suspected breaches (e.g., unauthorized access, data loss) should be reported immediately to the designated authority.
- Early detection minimizes damage and facilitates timely response.

Adherence to Access Controls:

- Employees should strictly adhere to access permissions based on their job roles.
- Least privilege principles apply to limit exposure.

BU Heads or Project Managers

Policy Enforcement:

- Management ensures consistent policy implementation across the organization.
- Regular audits verify compliance.

Resource Provision:

- Necessary resources, including training and tools, are provided to support compliance.
- Employees receive guidance on secure practices.

Monitoring Compliance:

- Regular checks ensure adherence to the policy.
- Violations trigger corrective actions.

CISO / Security/IT Team

Access Control Oversight:

- The IT department manages access control mechanisms.
- Proper authorization and role-based access are enforced.

Encryption and Monitoring Systems:

- IT professionals oversee encryption protocols (e.g., SSL/TLS) to protect data in transit.
- Continuous monitoring detects anomalies and potential breaches.

HR Team

- Overseeing the implementation and enforcement of this policy
- Create, Manage, Monitor, Maintain, Audit this Policy.

3) Scope

This policy applies to all departments, employees, contractors, and third-party service providers of [SecureCyberGates].

4) Definition of Confidential Information

4.1) Confidential Information

Confidential information refers to any data or information that is not publicly available and could potentially harm [SecureCyberGates]'s interests or those of its stakeholders if disclosed or misused. This includes, but is not limited to:

- Trade secrets and proprietary information
- Intellectual property, including patents, copyrights, and trademarks
- Financial data and projections
- Customer and client information
- Employee records, including personal and medical information
- Strategic plans and business strategies
- Pricing information and cost structures
- Research and development data
- Confidential contracts and agreements

4.2) Identifying Confidential Information

All confidential information should be clearly marked or identified as such. If the confidential nature of the information is not explicitly stated, employees should exercise caution and treat the information as confidential until its status is clarified.

4.3) Handling Confidential Information

Access to confidential information shall be granted on a need-to-know basis only. Employees are strictly prohibited from accessing, using, or disclosing confidential information without proper authorization and a legitimate business purpose.

4.4) Safeguarding and Storage

Employees must take appropriate measures to safeguard confidential information from unauthorized access, use, or disclosure. This includes:

- Securing physical documents in locked cabinets or rooms
- Encrypting electronic files and communications containing confidential information
- Using secure networks and communication channels
- Avoiding discussions of confidential information in public or insecure areas
- Properly disposing of confidential materials when no longer needed

4.4.1) Access Control

Separation of Duties:

- Different roles prevent unauthorized access.
- Users with specific responsibilities avoid overlapping duties.

Least Privilege:

- Users access only the minimum information required for their job functions.
- Reduces the risk of accidental or intentional data exposure.

User Access Management:

- Clearly defined procedures for granting, modifying, and revoking access rights.
- Secure protocols for remote access (e.g., VPNs).

4.4.2) Data Protection Measures

Encryption:

- All confidential data (both at rest and in transit) must be encrypted.
- Use secure cryptographic modules.

System Files:

- Secure system files and configurations to prevent unauthorized modifications.
- Protect against unauthorized access.

Development and Support:

- Ensure security during software development, maintenance, and support processes.
- Regularly assess and mitigate vulnerabilities.
- Follow secure coding practices.

4.4.3) Physical and Environmental Security

Secure Areas:

- Access controls for Server Room, offices, and storage facilities.
- Authorized personnel only.

Equipment Security:

- Safeguard servers, laptops, and other devices against theft or misuse.
- Implement physical security measures

4.4.4) Operations Security

Operational Procedures:

- Documented processes for data handling, backups, and maintenance.
- Consistent practices across the organization.

Malware Protection:

- Regularly update antivirus software.
- Educate employees about malware risks.

Logging and Monitoring:

- Monitor logs for security incidents.
- Detect anomalies and potential breaches.

Technical Vulnerability Management:

- Regularly apply patches.
- Conduct vulnerability scans.

4.4.5) Communications Security

Network Security:

- Implement network segmentation, firewalls, and intrusion detection systems.
- Protect against unauthorized access.

Information Transfer:

- Secure data transmission within [SecureCyberGates] and externally (e.g., encrypted emails).

4.4.6) Incident Management

- Promptly report any information security events or incidents.
- Investigate incidents, contain damage, and restore normal operations.
- Follow an incident response plan.

4.5) Disclosure and Sharing

Confidential information may only be disclosed or shared with authorized individuals or entities who have a legitimate business need for the information and have signed a non-disclosure agreement (NDA) or similar legally binding agreement.

4.6) Remote Access and Teleworking

Employees who access or handle confidential information remotely or while teleworking must adhere to the same security protocols and safeguards as when working on-site. Additional precautions, such as the use of virtual private networks (VPNs) and multi-factor authentication, may be required for remote access.

5) Confidentiality Agreements

As a prerequisite for employment at [SecureCyberGates] all employees are mandated to sign a confidentiality agreement. This legally binding agreement delineates the responsibilities of employees in safeguarding the company's confidential information and delineates the repercussions associated with any breaches or unauthorized disclosures of such information. This confidentiality agreement serves as a vital tool in upholding the integrity and security of sensitive data within the organization, ensuring that employees understand and fulfil their obligations in maintaining confidentiality and protecting the company's interests.

6) Third-Party Agreements

[SecureCyberGates] shall enter into non-disclosure agreements (NDAs) or similar legally binding agreements with third parties, such as contractors, consultants, vendors, and business partners, before sharing or granting access to confidential information.

7) Breaches of Confidentiality

Reporting Breaches

Employees are required to immediately report any suspected or known breaches of confidentiality to their immediate supervisor or the designated security officer. Prompt reporting is essential to mitigate potential harm and ensure appropriate action is taken.

Investigation and Corrective Action

All reported breaches will be thoroughly investigated by [SecureCyberGates]'s designated security team or appropriate authorities. Depending on the nature and severity of the breach, corrective actions may include disciplinary measures, legal action, or termination of employment or business relationships.

8) Employee Training and Awareness

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

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

9) Compliance and Monitoring

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

9.2) 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].

9.3) 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. [SecureCyberGates] reserves the right to conduct periodic audits and monitoring activities to ensure compliance with this policy and to identify potential vulnerabilities or risks. These activities may include but are not limited to:

- Access log reviews
- Network traffic monitoring
- Physical security checks
- Periodic policy compliance assessments
- Maintain records of compliance efforts.
- Comply with data protection laws (e.g., PDPA 2010).

10) Escalation Matrix

10.1) 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]

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

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

11) Policy Exceptions

11.1) 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]]**

12) Policy Review and Updates

12.1) 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.

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

12.3) 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.

12.4) 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.

13) Conclusion

[SecureCyberGates] is committed to maintaining the highest standards of confidentiality and ethical conduct. By adhering to this policy, [SecureCyberGates] can foster a culture of trust, protect our intellectual assets, and maintain our competitive advantage in the market. Every employee plays a crucial role in safeguarding confidential information, and their diligence and cooperation are essential for the successful implementation of this policy.

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