ENCRYPTION POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/ENCP/025/1.0
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

This Encryption Policy defines the requirements and guidelines for the use of encryption technologies to protect [SecureCyberGates]'s data and resources. Encryption is the process of encoding data or information in such a way that only authorized parties can access it, ensuring the confidentiality, integrity, and authenticity of the data.

Compliance with this policy is mandatory for all [SecureCyberGates] employees, contractors, vendors, and third-party service providers who have access to or handle [SecureCyberGates] 's data and resources.

The purpose of this policy is to:

- Protect the confidentiality, integrity, and authenticity of [SecureCyberGates] 's data and information assets.
- Ensure compliance with applicable laws, regulations, and industry standards, including SOC 2.
- Establish guidelines for the secure use of encryption technologies across all [SecureCyberGates] systems, applications, and communication channels.
- Define roles and responsibilities related to encryption implementation and management.

[SecureCyberGates] is committed to protecting the confidentiality, integrity, and availability of its data and information assets by implementing appropriate encryption controls. This policy outlines the requirements and guidelines for the use of encryption technologies, including the management of encryption keys, across all [SecureCyberGates] systems, applications, and communication channels.

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.
System administrators and application owners	1. Implementing and maintaining encryption controls in accordance with this policy. 2. Ensuring that encryption keys are properly managed and protected throughout their lifecycle. 3. Reporting any security incidents or potential breaches related to encryption to the Information Security Officer
Security Team	1. Responsible for ensuring Data backup requirements are in place. 2. Responsible for enforcing these requirements.

	3. Overseeing the implementation and enforcement of this policy. 4. Reviewing and approving encryption technologies, algorithms, and key management processes. 5. Providing guidance and support to [SecureCyberGates] employees and third-party service providers on encryption-related matters. 6. Conducting periodic reviews and audits to ensure compliance with this policy.
BU Heads or Project Managers	1. Ensuring that employees under their supervision comply with this policy. [Review and Approve this Policy]. 2. Each BU head must accept responsibility for ensuring critical data is stored on [SecureCyberGates] data processing systems and that those systems are being backed up. The BU head is also responsible for relaying the information about the criticality of the data to the [SecureCyberGates] IT Department.
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 encryption procedures. 4. Protecting encryption keys and sensitive data in accordance with established guidelines. 5. Reporting any suspected or actual security incidents related to encryption to the appropriate personnel.

3) Scope

This policy applies to all [SecureCyberGates] data and information assets, including but not limited to:

- Data stored on [SecureCyberGates] 's servers, databases, and storage systems (data at rest).
- Data transmitted over networks or communication channels (data in transit).
- Data stored on mobile devices, removable media, and endpoint devices.
- Encryption keys and key management processes.

4) Encryption Requirements

4.1) Data at Rest

[SecureCyberGates] shall implement appropriate encryption controls to protect data stored on servers, databases, storage systems, and endpoint devices (data at rest). The following requirements shall be met:

Full Disk Encryption (FDE): All laptops, desktops, and mobile devices used by [SecureCyberGates] employees or authorized third parties must have Full Disk Encryption (FDE) enabled, using industry-standard encryption algorithms and key strengths (e.g., AES-256).

Database and Storage Encryption: All databases and storage systems containing sensitive or confidential data must be encrypted using industry-standard encryption algorithms and key strengths (e.g., AES-256).

Backup Encryption: All backup media containing sensitive or confidential data must be encrypted using industry-standard encryption algorithms and key strengths (e.g., AES-256).

Removable Media Encryption: Sensitive or confidential data stored on removable media (e.g., USB drives, external hard drives) must be encrypted using industry-standard encryption algorithms and key strengths (e.g., AES-256).

Cloud Storage Encryption: Any sensitive or confidential data stored in cloud storage services must be encrypted using industry-standard encryption algorithms and key strengths (e.g., AES-256).

Key Management: Encryption keys for data at rest must be securely managed and protected throughout their lifecycle, in accordance with the Key Management section of this policy.

4.2) Data in Transit

[SecureCyberGates] shall implement appropriate encryption controls to protect data transmitted over networks or communication channels (data in transit). The following requirements shall be met:

Secure Network Protocols: All data transmitted over internal and external networks must be encrypted using secure network protocols, such as Transport Layer Security (TLS) or Internet Protocol Security (IPsec), with industry-standard encryption algorithms and key strengths (e.g., AES-256, RSA-2048).

Virtual Private Network (VPN): [SecureCyberGates] employees and authorized third parties accessing [SecureCyberGates]'s internal network or resources from remote locations must use a Virtual Private Network (VPN) with appropriate encryption controls (e.g., AES-256, RSA-2048).

Email Encryption: Sensitive or confidential data transmitted via email must be encrypted using industry-standard email encryption solutions (e.g., S/MIME, PGP).

File Transfer Encryption: Sensitive or confidential data transferred between [SecureCyberGates] and third parties must be encrypted using secure file transfer protocols (e.g., SFTP, HTTPS) with industry-standard encryption algorithms and key strengths (e.g., AES-256, RSA-2048).

Key Management: Encryption keys for data in transit must be securely managed and protected throughout their lifecycle, in accordance with the Key Management section of this policy.

With the goals of protecting private and confidential data and enhancing security, [SecureCyberGates] encrypts all data & data communications. All passwords are either encrypted using AES-256 or hashed with SHA-512 with SALT. Password encryption also supports one-way hash using BCRYPT. Data in transit is encrypted on TLS 1.2 and TLS 1.3 while Data at Rest uses AES256.

4.3) Cryptographic Algorithms and Key Strengths

[SecureCyberGates] shall use industry-standard and approved cryptographic algorithms and key strengths for encryption, as recommended by recognized organizations . The following guidelines shall be followed:

Symmetric Encryption Algorithms: AES-256 or higher shall be used for symmetric encryption of data at rest and data in transit.

Asymmetric Encryption Algorithms: RSA-2048 or higher, or elliptic curve cryptography (ECC) with equivalent or higher key strengths, shall be used for asymmetric encryption and key exchange.

Hashing Algorithms: SHA-256 or higher shall be used for hashing and message authentication.

Key Exchange Protocols: Secure key exchange protocols, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman, shall be used for establishing shared secrets and exchanging encryption keys.

Regular Review: Cryptographic algorithms and key strengths shall be reviewed regularly and updated as necessary to address potential vulnerabilities and maintain adequate protection.

4.4) Key Management

[SecureCyberGates] uses cloud provider's key management service to store and manage encryption keys and secrets that facilitate secure access to resources. As part of key life cycle management, the services from major public cloud providers allow the rotation of keys to generate new cryptographic material. Key management services from all major cloud providers allow for both customer managed keys and cloud provider managed keys

[SecureCyberGates] shall implement a comprehensive key management process to ensure the secure generation, storage, distribution, and disposal of encryption keys. The following requirements shall be met:

Key Generation: Encryption keys shall be generated using secure, random, and unpredictable methods, approved by recognized organizations.

Key Storage: Encryption keys shall be stored securely, either in hardware security modules (HSMs) or encrypted using industry-standard encryption algorithms and key strengths.

Key Distribution: Encryption keys shall be distributed securely using industry-standard key exchange protocols and secure communication channels.

Key Access Control: Access to encryption keys shall be restricted based on the principle of least privilege and separated roles and responsibilities.

Key Rotation and Expiration: Encryption keys shall be rotated and expired periodically, in accordance with industry best practices and the sensitivity of the data being protected.

Key Backup and Recovery: Encryption keys shall be backed up and recoverable in case of system failures or other incidents, while maintaining appropriate access controls and audit trails.

Key Destruction: Encryption keys shall be securely destroyed or revoked when no longer needed, using approved methods to prevent unauthorized access or recovery.

Key Management Documentation: A comprehensive key management plan shall be documented, detailing the processes and procedures for all stages of the key lifecycle, including generation, storage, distribution, rotation, backup, and destruction.

Key Management Roles and Responsibilities: Clear roles and responsibilities shall be defined for individuals involved in the key management process, including key custodians, key administrators, and key recovery personnel.

Key Management Auditing and Monitoring: Key management activities shall be audited and monitored to detect and prevent unauthorized access, modifications, or misuse of

encryption keys.

Key Management Training: [SecureCyberGates] shall provide regular training and awareness programs for personnel involved in key management processes to ensure they understand and follow established procedures and best practices.

5) Encryption for Third-Party Services and Cloud Providers

When leveraging third-party services or cloud providers for storing, processing, or transmitting [SecureCyberGates]'s data, the following requirements shall be met:

Encryption Requirements: Third-party services and cloud providers must meet or exceed [SecureCyberGates]'s encryption requirements as outlined in this policy.

Encryption Key Management: [SecureCyberGates] shall retain control and ownership of encryption keys whenever possible. If encryption keys are managed by the third-party or cloud provider, their key management processes must be reviewed and approved by [SecureCyberGates]'s Information Security Officer

Data Residency and Compliance: [SecureCyberGates] shall ensure that the third-party service or cloud provider complies with applicable data residency and regulatory requirements related to encryption and data protection.

Due Diligence and Risk Assessment: [SecureCyberGates] shall conduct due diligence and risk assessments on third-party services and cloud providers to ensure their encryption and data protection practices align with [SecureCyberGates]'s security requirements and industry best practices.

6) Encryption for Mobile Devices and Remote Access

[SecureCyberGates] shall implement appropriate encryption controls for mobile devices and remote access to ensure the protection of sensitive or confidential data. The following requirements shall be met:

Mobile Device Encryption: All mobile devices (e.g., laptops, tablets, smartphones) used to access, store, or process [SecureCyberGates]'s data must have Full Disk Encryption (FDE) or equivalent encryption controls enabled, using industry-standard encryption algorithms and key strengths.

Remote Access Encryption: Remote access to [SecureCyberGates]'s internal network or

resources must be secured using Virtual Private Network (VPN) technologies with appropriate encryption controls, in accordance with the Data in Transit section of this policy.

Secure Communication Channels: Communication channels used for remote access or mobile device management must be encrypted using industry-standard protocols and encryption algorithms, as specified in the Data in Transit section of this policy.

Mobile Device Management: [SecureCyberGates] shall implement a Mobile Device Management (MDM) solution to monitor and enforce encryption and other security controls on mobile devices used for business purposes. Data stored on mobile devices must be encrypted to protect it in case of loss or theft. Encryption must be applied to both the device's storage and external storage media.

7) Encryption for Sensitive Data

[SecureCyberGates] shall implement additional encryption controls for sensitive or high-risk data, such as personally identifiable information (PII), financial data, and intellectual property. The following requirements shall be met:

Data Classification: [SecureCyberGates] shall establish a data classification program to identify and classify sensitive or high-risk data based on its sensitivity and potential impact on the organization.

Encryption Requirements: Sensitive or high-risk data shall be encrypted using industry-standard encryption algorithms and key strengths, in accordance with the Data at Rest and Data in Transit sections of this policy.

Access Controls: Access to sensitive or high-risk data shall be restricted based on the principle of least privilege and separated roles and responsibilities.

Monitoring and Auditing: Access and usage of sensitive or high-risk data shall be monitored and audited to detect and prevent unauthorized access or misuse.

Data Masking and Tokenization: [SecureCyberGates] shall consider implementing data masking or tokenization techniques to protect sensitive or high-risk data in non-production environments or when sharing data with third parties.

Regulatory Compliance: [SecureCyberGates] shall ensure that encryption controls for sensitive or high-risk data comply with applicable laws, regulations, and industry standards, such as the PDPA, Payment Card Industry Data Security Standard (PCI DSS). Highly confidential data must be encrypted in transit and at rest with the strongest encryption protocols and key management. Transparent Data Encryption or Tokenization is required for column level encryption.

8) Encryption for Backups and Archives

[SecureCyberGates] shall implement appropriate encryption controls to protect backups and archives containing sensitive or confidential data. The following requirements shall be met:

Backup Encryption: All backup media containing sensitive or confidential data must be encrypted using industry-standard encryption algorithms and key strengths, as specified in the Data at Rest section of this policy.

Offsite Backup Encryption: Offsite backups or archives containing sensitive or confidential data must be encrypted during transmission and storage, using industry-standard encryption algorithms and key strengths.

Backup Key Management: Encryption keys used for backup encryption shall be securely managed and protected throughout their lifecycle, in accordance with the Key Management section of this policy.

Backup Monitoring and Auditing: Backup and archive activities involving sensitive or confidential data shall be monitored and audited to detect and prevent unauthorized access or misuse.

Backup Media Handling and Disposal: Backup media containing sensitive or confidential data shall be handled and disposed of securely, in accordance with [SecureCyberGates]'s data handling and disposal policies.

9) Encryption for Email and File Transfers

Procedures must be defined and employed for monitoring backup jobs, times, data volumes and success rates of backup activities. This data must be assembled for tracking reasons and for evaluation of compliancy for established service level agreements, business processing objectives, etc. Additionally, procedures need to be implemented for monitoring, reporting and tracking of problems that occur during the backup process.
[SecureCyberGates] shall implement appropriate encryption controls to protect sensitive or confidential data transmitted via email or file transfers. The following requirements shall be met:

Email Encryption: Sensitive or confidential data transmitted via email must be encrypted using industry-standard email encryption solutions, such as S/MIME or PGP, with appropriate encryption algorithms and key strengths.

File Transfer Encryption: Sensitive or confidential data transferred between [SecureCyberGates] and third parties must be encrypted using secure file transfer protocols, such as SFTP or HTTPS, with industry-standard encryption algorithms and key strengths.

Email and File Transfer Monitoring: Email and file transfer activities involving sensitive or confidential data shall be monitored and audited to detect and prevent unauthorized access or misuse.

Email and File Transfer Policies: [SecureCyberGates] shall establish policies and procedures for the secure handling and transmission of sensitive or confidential data via email and file transfers, including guidelines for encryption, access controls, and incident response.

10) Encryption for Cloud Services and Infrastructure

Regulatory requirements stipulating data retention and protection requirements must be evaluated and included when developing data backup and retention schedules.
[SecureCyberGates] shall implement appropriate encryption controls for cloud services and infrastructure to ensure the protection of sensitive or confidential data. The following requirements shall be met:

Cloud Encryption: Sensitive or confidential data stored or processed in cloud services or infrastructure must be encrypted using industry-standard encryption algorithms and key strengths, as specified in the Data at Rest and Data in Transit sections of this policy. Data at rest and in transit in cloud environments will be encrypted using strong encryption algorithms (at least AES256 for data at rest and TLS v1.2 for data in transit).

Cloud Key Management: [SecureCyberGates] shall retain control and ownership of encryption keys for cloud services and infrastructure whenever possible. If encryption keys are managed by the cloud service provider, their key management processes must be reviewed and approved by [SecureCyberGates]'s Information Security Officer. Encryption keys will be securely managed and rotated as necessary.

Cloud Access Controls: Access to cloud services and infrastructure containing sensitive or confidential data shall be restricted based on the principle of least privilege and separated roles and responsibilities.

Cloud Monitoring and Auditing: Activities related to cloud services and infrastructure containing sensitive or confidential data shall be monitored and audited to detect and prevent unauthorized access or misuse.

Cloud Service Provider Assessments: [SecureCyberGates] shall conduct regular assessments and due diligence on cloud service providers to ensure their encryption and data protection practices align with [SecureCyberGates]'s security requirements and industry best practices.

Cloud Compliance: [SecureCyberGates] shall ensure that the use of cloud services and infrastructure complies with applicable laws, regulations, and industry standards related to data protection and encryption. If PCI DSS compliance is required, Transparent Data Encryption or tokenization must be used.

11) Encryption for Endpoint Protection

[SecureCyberGates] shall implement appropriate encryption controls for endpoint devices, such as laptops, desktops, and mobile devices, to ensure the protection of sensitive or confidential data. The following requirements shall be met:

Full Disk Encryption (FDE): All endpoint devices used by [SecureCyberGates] employees or authorized third parties must have Full Disk Encryption (FDE) enabled, using industry-standard encryption algorithms and key strengths, as specified in the Data at Rest section of this policy.

Removable Media Encryption: Sensitive or confidential data stored on removable media (e.g., USB drives, external hard drives) used with endpoint devices must be encrypted using industry-standard encryption algorithms and key strengths.

Endpoint Device Access Controls: Access to endpoint devices containing sensitive or confidential data shall be restricted based on the principle of least privilege and separated roles and responsibilities.

Endpoint Device Monitoring and Auditing: Activities related to endpoint devices containing sensitive or confidential data shall be monitored and audited to detect and prevent unauthorized access or misuse.

Endpoint Device Management: [SecureCyberGates] shall implement a centralized endpoint management solution to enforce encryption and other security controls on endpoint devices used for business purposes.

Endpoint Device Hardening: Endpoint devices shall be hardened and configured according to industry best practices and 's security standards.

12) Encryption for Development and Testing Environments

[SecureCyberGates] shall implement appropriate encryption controls for development and testing environments to ensure the protection of sensitive or confidential data used for non-production purposes. The following requirements shall be met:

Development and Testing Data Encryption: Sensitive or confidential data used in development and testing environments must be encrypted using industry-standard encryption algorithms and key strengths, as specified in the Data at Rest and Data in Transit sections of this policy.

Development and Testing Key Management: Encryption keys used for development and testing environments shall be securely managed and protected throughout their lifecycle, in accordance with the Key Management section of this policy.

Development and Testing Access Controls: Access to development and testing environments containing sensitive or confidential data shall be restricted based on the principle of least privilege and separated roles and responsibilities.

Development and Testing Monitoring and Auditing: Activities related to development and testing environments containing sensitive or confidential data shall be monitored and audited to detect and prevent unauthorized access or misuse.

Development and Testing Data Masking and Tokenization: [SecureCyberGates] shall consider implementing data masking or tokenization techniques to protect sensitive or confidential data in development and testing environments.

Development and Testing Environment Separation: Development and testing environments shall be logically or physically separated from production environments to prevent accidental exposure or misuse of sensitive or confidential data.

13) Encryption for Remote Access and Virtual Private Networks (VPNs)

[SecureCyberGates] shall implement appropriate encryption controls for remote access and Virtual Private Network (VPN) connections to ensure the protection of sensitive or confidential data. The following requirements shall be met:

VPN Encryption: All VPN connections used for remote access to [SecureCyberGates]'s

internal network or resources must be secured using industry-standard encryption algorithms and key strengths, as specified in the Data in Transit section of this policy. Wireless networks must use WPA2 (or a more secure protocol) to enforce both authentication and encryption

VPN Authentication: VPN connections shall require strong authentication mechanisms, such as multi-factor authentication (MFA) or digital certificates, to prevent unauthorized access.

VPN Monitoring and Auditing: VPN activities shall be monitored and audited to detect and prevent unauthorized access or misuse.

VPN Access Controls: Access to VPN connections shall be restricted based on the principle of least privilege and separated roles and responsibilities.

VPN Configuration and Hardening: VPN servers and clients shall be configured and hardened according to industry best practices and [SecureCyberGates]'s security standards.

VPN Key Management: Encryption keys used for VPN connections shall be securely managed and protected throughout their lifecycle, in accordance with the Key Management section of this policy.

14) Employee Training and Awareness

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

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

15) Compliance and Monitoring

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

15.2) 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].

15.3) 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 password security policy.

15.4) Procedures must be defined and employed for monitoring backup jobs, times, data volumes and success rates of backup activities. This data must be assembled for tracking reasons and for evaluation of compliancy for established service level agreements, business processing objectives, etc. Additionally, procedures need to be implemented for monitoring, reporting and tracking of problems that occur during the backup process.

16) Escalation Matrix

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

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

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

17) Policy Exceptions

17.1) 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]]**

18) Policy Review and Updates

18.1) 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.

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

18.3) 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.

18.4) 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.

19) Conclusion

[SecureCyberGates] is committed to protecting the confidentiality, integrity, and availability of its data and information assets through the implementation of appropriate encryption controls. This Encryption Policy provides a comprehensive framework for the secure use of encryption technologies across all [SecureCyberGates] systems, applications, and communication channels.

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.

[SecureCyberGates] recognizes that encryption is a critical component of its overall information security strategy and will continue to review and update this policy as necessary to address emerging threats, technological advancements, and evolving business needs.

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