NETWORK SECURITY POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/NWSP/023/1.0
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 policy provides comprehensive guidance for implementing network security controls to safeguard the integrity, confidentiality, and availability of [SecureCyberGates]'s networks.

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 Team / Security Team	1. Responsible for ensuring Network Security requirements are in place. 2. Responsible for enforcing these requirements. 3. IT Team is primarily responsible for the effective implementation and ongoing maintenance of this network security procedure. Additionally, IT team lead and the Information Security Officer assumes the role of approving and periodically reviewing this procedure to ensure its continued relevance and effectiveness.
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

This procedure applies to all networks and network devices utilized within [SecureCyberGates]'s infrastructure.

4) Network Security Management

4.1) Network Controls

- Utilize a combination of firewalls, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), encryption, and other robust controls to fortify the security posture of [SecureCyberGates] 's networks.

- All modifications or updates to network configurations must comply with the established change management process to maintain consistency and integrity.
- Regularly **monitor network logs** to promptly identify and respond to security events, ensuring timely mitigation of potential threats.
- Conduct thorough **annual vulnerability scans and penetration tests** to identify and address any weaknesses or vulnerabilities in the network infrastructure.

4.2) Network Access

- Implement stringent access controls to restrict access to production networks based on the principle of least privilege, ensuring that only authorized personnel have access to sensitive resources.
- Maintain a comprehensive list of authorized users with access to production networks, regularly reviewing and updating it to reflect current personnel and access requirements.
- Permit remote access exclusively through encrypted protocols to uphold data confidentiality and mitigate the risk of unauthorized access.

4.3) Network Segmentation

- Employ robust network segmentation techniques, such as Virtual Private Clouds (VPCs) or subnets, to isolate and compartmentalize network resources based on trust levels and security requirements.
- Implement strict traffic control measures between network zones using gateways and firewalls to prevent unauthorized access and mitigate the spread of potential threats.
- Provide internet access through designated public subnets, governed by predefined user roles and access policies to ensure secure and controlled connectivity.

4.4) Remote Devices

- Enforce stringent security measures for all remote devices, including the installation and maintenance of updated anti-virus software and firewalls to mitigate the risk of malware infections and unauthorized access.
- Conduct regular employee training and awareness programs to educate personnel about the risks associated with connecting to public Wi-Fi networks without adequate firewall protection, emphasizing the importance of adhering to security best practices.

Security Control	Description
Network Firewall Rule sets	[SecureCyberGates] has a set of objectives in order to ensure security levels are met. This includes regularly tracking and monitoring for suspicious activity via firewall reports and monthly audit reviews. We take a zero-trust approach whereby all security lists and network groups deny all traffic by default. Configurations allow traffic on a need-to-have basis. Also,

	these policies are reviewed on a quarterly basis.
Intrusion Detection and prevention	For cloud services, the cloud service provider's threat detection service will be subscribed to. If another data center is used for collocation, ensure that Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are installed.
Web Application Firewall (WAF)	All [SecureCyberGates] solutions have our inbuilt secure guard web application firewall. In addition to this, for solutions where there is a public facing module, a Web Application Firewall (WAF) will be implemented to protect from various threats. The WAF will cover all externally accessible web applications and APIs. WAF rule sets will be configured to detect and block common web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), and remote file inclusion.
Wireless Network Security	Wireless networks must use WPA2 (or a more secure protocol) to enforce both authentication and encryption. Wireless network traffic will be segmented to ensure that sensitive data is isolated from guest networks and Firewall rules will be defined to restrict access between segments. Access control lists (ACLs) will be implemented to control who can connect to the wireless network, utilizing the principle of least privilege will be applied to restrict access based on job responsibilities. Annual wireless network vulnerability assessments and penetration tests will be conducted.

5) Employee Training and Awareness

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

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

6) Compliance and Monitoring

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

6.2) 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].

6.3) 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.

7) Escalation Matrix

7.1) 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]

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

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

8) Policy Exceptions

8.1) 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]]**

9) Policy Review and Updates

9.1) 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.

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

9.3) 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.

9.4) 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.

10) Conclusion

By implementing and adhering to this policy, [SecureCyberGates] aims to secure Company network infrastructure 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