ENDPOINT SECURITY POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/ENDP/026/1.0
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

Our Endpoint Security Policy serves as guidance for ensuring that risks related to endpoint devices (laptops, desktops, mobile devices, etc.) used to access company systems and data are properly identified, assessed, and mitigated. Since the information security team facilitates and provides advisory on endpoint security risk management, all business units and users of endpoint devices are expected to be active participants in [SecureCyberGates] 's endpoint risk discussions.

This Endpoint Security Policy establishes the standards that promote effective management of endpoint risks at the appropriate level within the organization, which is critical for [SecureCyberGates]'s long-term success and protection of its information assets. Therefore, [SecureCyberGates] shall periodically assess the risks associated with the use of endpoint devices for processing, storing, or transmitting sensitive information to support business processes and take appropriate action to mitigate unacceptable risks.

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 Endpoint 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

It is important to note that this Endpoint Security Policy may not cover every possible scenario; if you are unsure how the standards or guidelines apply in a given situation, please seek further guidance from the the IT team, Security team, or the relevant business unit managers.
Each individual is responsible for ensuring compliance with these guidelines, and all stakeholders will be held accountable for upholding their commitments to this Endpoint Security Policy.

4) Endpoint Security Policy

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

4.1) Objective

[SecureCyberGates] develops, implements, and governs processes and documentation to facilitate an enterprise-wide risk management program for endpoint security.

4.2) Standard

[SecureCyberGates] is required to develop and implement an enterprise-wide endpoint security risk management strategy that includes:
a) A formal risk assessment performed at least annually and upon significant changes to the environment (e.g., acquisition, merger, relocation).
b) Identification of critical endpoint assets, current safeguards, effectiveness of safeguards, threats, and vulnerabilities.
c) Review of processes involving endpoint devices used for creating, receiving, maintaining, and transmitting sensitive data.
d) Assigning responsibility to validate endpoint security controls.

4.3) Guidelines

The endpoint security and antivirus risk management strategy at [SecureCyberGates] should include:

a) An unambiguous expression of the organization's risk tolerance for threats related to endpoints and malware.
b) Risk mitigation strategies and controls to reduce risks to endpoints from unauthorized access, malware infections, data breaches etc. to an acceptable level based on the risk tolerance.
c) A consistent process for periodically evaluating endpoint security posture, antivirus capabilities, emerging threats, and monitoring risks over time.
d) Criteria and thresholds for determining when risks related to new malware, vulnerabilities in endpoints/antivirus, gaps in existing controls etc. are unacceptable and require risk treatment.

Risk treatment options like implementing new security controls, antivirus solution upgrades,

refreshing endpoint hardware, increasing user awareness etc. to mitigate unacceptable risks.

4.4) Procedures

IT Team, Security Team will:

a) Use vendor-recommended settings and secure practices to ensure sufficient controls for managing endpoint risks, including:

I. A formal Risk Management Program (RMP) covering risk tolerance, assessment methodologies, and mitigation strategies.

II. A process for consistently evaluating and monitoring endpoint risks.

III. A process for annual risk assessments and assessments upon significant environment changes.

IV. Identification of critical endpoint assets, safeguards, threats, and vulnerabilities.

V. Review of processes involving sensitive data on endpoints.

VI. Assigning responsibility for validating endpoint security controls.

b) Annually in the first quarter, review processes for non-conformance and revise as needed.

I. Distribute process changes to key personnel.

II. Communicate changes to key personnel.

c) Request corrective actions to address identified deficiencies.

d) Validate that corrective actions occurred to remediate deficiencies.

e) Document results of corrective actions and note findings.

f) Request additional corrective actions for non remediated deficiencies.

This policy provides an overview of the Risk Management Program for endpoint security at [SecureCyberGates]. All employees, contractors and third parties are expected to comply with this policy and associated procedures.

5) Policy Statements

5.1 Endpoint Device Security

a) All endpoint devices must have company-approved and centrally managed antivirus software installed before being granted network access.

b) Full disk encryption must be enabled on endpoints using authorized encryption software/features.

c) Automatic screen lock must be configured after a maximum of 15 minutes of inactivity.

d) Only strong passwords that comply with the Password Policy requirements are permitted.

e) Software patches and updates for operating systems and applications must be installed promptly.

f) Only IT-approved applications can be installed on endpoints. No unauthorized software is permitted.

g) All users should have non administrative priveleges on Company owned devices.

5.2 Anti-Malware Solution

An effective anti-malware solution will be deployed across all endpoints, servers, and network gateways. The solution will include real-time scanning, signature-based detection, and behavior-based analysis. If the solution is hosted on a cloud environment the provider's anti malware solution should be subscribed to. If no anti malware service is available, Security recommended anti malware solution should be installed on every endpoint. [SecureCyberGates] uses **McAfee** Endpoint Security Cloud for company managed devices.

5.3 User Responsibilities

a) Ensure antivirus is running, active and updating properly on assigned endpoints.
b) Do not disable, uninstall or stop the centralized antivirus software under any circumstances.
c) Do not open or execute any untrusted attachments, links or software on endpoints.
d) Report suspected malware security incidents to security@securecybergates.com immediately.
e) Allow IT teams to access endpoints for ensuring policy compliance and incident response.
f) Remote users are responsible for ensuring their devices are free from malware.

5.4 Incident Handling

a) Devices suspected of malware infection will be immediately isolated from the corporate network.
b) IT will follow antivirus vendor-recommended practices to clean and disinfect the infected device.
c) Devices with unremovable malware infections will be re-imaged or remain in quarantine.
d) Backup and data recovery procedures will be followed for impacted endpoints as needed.

6) Employee Training and Awareness

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

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

7) Compliance and Monitoring

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

7.2) 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].

7.3) 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.

8) Escalation Matrix

8.1) 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]

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

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

9) Policy Exceptions

9.1) 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]]**

10) Policy Review and Updates

10.1) 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.

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

10.3) 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.

10.4) 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.

11) Conclusion

[SecureCyberGates] is committed to protecting the confidentiality, integrity, and availability of its data and information assets through the implementation of appropriate Endpoint 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

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