PHYSICAL SECURITY POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/PSP/007/1.0
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

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 Physical Security Policy establishes the standards that promote fairness in implementing appropriate physical access controls to safeguard humans, limit access to Assets[systems, equipment, and the respective operating environments] to authorized individuals.[SecureCyberGates]shall provide appropriate environmental controls in facilities containing systems to ensure sufficient environmental conditions exist to promote Human Safety ,avoid preventable hardware failures and service interruptions.

This Policy applies to anyone who conducts business for or on behalf of [SecureCyberGates]and have physical access to [SecureCyberGates]premise including:

1. All employees / Contractors
2. Management and company owners
3. External business partners who act on [SecureCyberGates]'s behalf or in our interest as Third Party Representatives

It is important to note that every situation may not be addressed in this Physical Security Policy; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from the IT team , Security Team.
Each and every one of us are responsible for ensuring that we follow these guidelines, and we will be held accountable for upholding our commitments to this Physical Security Policy.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Overseeing the implementation and enforcement of this policy [Review and Approve Physical Security Policy]
IT/Security Team	Create, Manage, Monitor, Maintain, Audit Physical Security Policy
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review and Approve Physical Security Policy]
Employees / Contractors	1. Read this Physical Security Policy 2. Ask questions / Provide Feedbacks 3. Report possible or actual violations of this Physical Security Policy.

3) Scope

This policy applies to all individuals, including employees, contractors, vendors, and third-

party users, who have been granted access to any [SecureCyberGates] Premise [Physical Office Location] OR Remote Working Locations.This policy covers all types of Physical Locations, Handling of Physical Assets [e.g. USB , Laptop , Desktop , Papers [Physical Print Copies] used within [SecureCyberGates]'s physical office environments. This policy is also applicable for [SecureCyberGates] employees, contractors working from Remote Locations and DOES NOT have Physical access to [SecureCyberGates] Premise.

4) Physical access Control

4.1) Control Objective

The organization:

1. Enforces physical access authorizations for all physical access points (including designated entry / exit points) to the facility where the system resides (excluding those areas within the facility officially designated as publicly accessible).
2. Verifies individual access authorizations before granting access to the facility.
3. Controls entry to the facility containing the system using physical access devices and / or guards.
4. Controls access to areas officially designated as publicly accessible in accordance with [SecureCyberGates]'s assessment of risk.
5. Secures keys, combinations, and other physical access devices.
6. Changes combinations and keys and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

4.2) Standard

Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard Humans, sensitive data and systems.

This includes, but is not limited to:

1. Use video cameras and / or access control mechanisms to limit and monitor physical access to the facility and systems.
2. Enforce physical access authorizations for all physical access points (including designated entry / exit points) to company-owned or operated facilities.
3. Verify individual access authorizations before granting access to the facility.
4. Control access to areas based on the physical security zone requirements.
5. Secure keys, combinations, and other physical access devices.
6. Change combinations and keys and when keys are lost, combinations are compromised or when individuals are transferred or terminated.

7. Issue visitors a physical token (e.g., a badge or access device) that:
   7.1 Identifies the visitors as not onsite personnel.
   7.2 Must be surrendered before leaving the facility or at the date of expiration.
   7.3 Expires through automated or visual means (e.g., different color for each day).

4.3) Guidelines

This applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.

Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected systems / components in secured areas. Components of systems (e.g., workstations, computer terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.

4.4) Procedure

Control Activity:

In house IT Team and Security Team:

1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for managing risk that includes:

1.1 A formal Risk Management Program that includes:

- An unambiguous expression of the risk tolerance.
- Acceptable risk assessment methodologies.
- Risk mitigation strategies.

1.2 A process for consistently evaluating and monitoring risk over time.

1.3 A process for conducting risk assessments annually and upon significant changes to the corporate environment (e.g., acquisition, merger, relocation).

1.4 Identification of:

- Critical assets.
- Current safeguards.
- Effectiveness of safeguards, threats, and vulnerabilities.

1.5 Reviewing processes involving creating, receiving, maintaining, and transmitting of sensitive data.

1.6 Assigning responsibility to validate security controls

2) On at least an annual basis, during the 1st quarter of the calendar year, reviews the process for non-conforming instances. As needed, revise processes to address necessary changes and evolving conditions. Whenever the process is updated:
    - Distributes copies of the change to key personnel.
    - Communicates the changes and updates to key personnel.

3) If necessary, requests corrective action to address identified deficiencies.
4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
5) If necessary, document the results of corrective action and note findings.
6) If necessary, requests additional corrective action to address un-remediated deficiencies.

5) Monitoring Physical access

5.1) Control Objective

The organization:
- Monitors physical access to detect and respond to physical security incidents.
- Reviews physical access logs.
- Coordinates results of reviews and investigations with [SecureCyberGates]'s incident response capability[Security Team].

5.2) Standard

[SecureCyberGates] is responsible for:

1) Investigating and responding to detected physical security incidents, per documented procedures.
2) Performing security checks at the physical boundary of the facility or system for unauthorized exfiltration of information or system components.
3) Using video cameras and / or access control mechanisms to monitor individual physical access to sensitive areas.
4) Reviewing collected data and correlate with other entries.

5) Retaining physical access data for **at least three (3) months**, unless otherwise restricted by law.

5.3) Guidelines
None

5.4) Procedure
None

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 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 Physical security policy. These audits may include, but are not limited to:

- Reviewing Physical Security Controls are working [e.g. Door Locks , CCTV Footage etc.]
- Ensuring Fire Detection and Prevention systems are working [Building Security]

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 Physical Security 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 maintaining the highest standards for Physical security. Every employee plays a crucial role in safeguarding confidential information, and their diligence and cooperation are essential for the successful implementation of this policy.

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