ASSET MANAGEMENT POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/ASMP/027/1.0
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

SECURE CYBER GATES

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 6

2) Roles &Responsibilities 6

3) Scope 6

4) Asset Inventories 7

4.1) Control Objective 7

4.2) Standard 7

4.3) Guidelines 7

4.4) Comprehensive Asset Registry 7

4.5) Asset Identification 8

4.6) Ownership Assignment 8

4.7) Asset Classification 8

4.8) Asset Categorization 8

4.9) Asset Register 9

4.10) Asset Relocation/Transfer 9

5) Employee Training and Awareness 9

6) Compliance and Monitoring 9

7) Escalation Matrix 10

8) Policy Exceptions 10

9) Policy Review and Updates 10

10) Conclusion 11

1) Objective

Our Asset Management Policy serves as guidance for ensuring that technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal. This Asset Management Policy establishes the standards that promote fairness in protecting its assets and data by implementing and maintaining appropriate IT Asset Management business practices across the enterprise.

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 Asset management 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 every situation may not be addressed in this Asset Management Policy; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from the Security or IT 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 Asset Management Policy.

4) Asset Inventories

All assets including but not limited to laptops, displays, storage etc are tagged and documented. An up-to-date inventory and asset control is maintained to ensure efficient tracking of equipment.

Our intellectual property is tracked internally by our legal compliance team. We also track third-party licenses, compliance with licenses, compliance with data privacy requirements of customers and acceptable usage of data.

4.1) Control Objective

The organization develops, documents, and maintains an inventory of system components that: Valid access authorization from the immediate supervisor or system owner.

- Accurately reflects the current system;
- Is at the level of granularity deemed necessary for tracking and reporting;
- Includes organization-defined information deemed necessary to achieve effective property accountability; and
- Is available for review and audit by designated organizational officials.

4.2) Standard

[SecureCyberGates] is required to maintain an inventory of its technology assets that includes, but is not limited to:

- Hardware and software inventories, both:
  Internally hosted assets and
  Externally hosted assets;
- A method to accurately and readily determine owner, contact information and purpose (e.g., labelling, coding, and / or inventorying of devices);
- List of company-approved products;
- Updating the inventory as necessary.

4.3) Guidelines

The inventory should be updated as an integral part of component installations, removals, and system updates. Without an inventory, some system components could be forgotten and be inadvertently excluded from applicable configuration standards. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to [SecureCyberGates] network.

4.4) Comprehensive Asset Registry

A comprehensive asset inventory will be maintained by **IT Team** to document all IT hardware, software, and information assets. The registry will include asset names, unique identifiers, descriptions, and ownership details.

4.5) Asset Identification

All assets will be uniquely identified to distinguish them from one another with a unique identifier, asset tag or serial number.

4.6) Ownership Assignment

Asset ownership will be assigned to individuals or teams responsible for the management, security, and maintenance of specific assets. The owners will be identified and documented in the asset registry, and they are responsible for safeguarding their assets, ensuring compliance with security policies and standards and overseeing access control, patch management, and maintenance.

4.7) Asset Classification

Data assets within [SecureCyberGates] are classified based on their **sensitivity and importance**. This exercise guides classification will guide access controls, encryption, and data handling procedures. Assets would be classified in 4 types similar to Data classification :

Classification Type	Description
Public Asset	Asset of Company accessible to Common Public.
Internal Asset	Asset of Company accessible to ALL Internal Employees / Contractors.
Confidential Asset	Asset of Company accessible a Project / Team [ALL Internal Employees / Contractors Does NOT have access]
Restricted / Highly Confidential Asset	Asset of Company accessible ONLY Some individuals [NOT entire Project/Team] [e.g. Productional Server]

4.8) Asset Categorization

IT hardware and software assets will be categorized based on their criticality and relevance to business operations. Categorization will inform asset management practices. Some categorization examples are

Categorization Type	Description
Hardware Asset	This includes physical components like computers, servers, networking equipment, printers, and other devices.
Software Asset	This category covers operating systems, applications, databases, and other software licenses.
HR Assets	All Assets used by HR team.
“BANK ABC” Assets	All Assets used by “BANK ABC” Project.
Development Assets	All Assets used for Development environment activities
SIT Assets	All Assets used for SIT environment activities
UAT Assets	All Assets used for UAT environment activities

PROD Assets	All Assets used for PRODUCTION environment activities

Categorization are providing Tags / Labells to Assets for better management, **One Asset may have multiple such Labels.**
E.g. A Physical Production Server for Bank ABC
[Labels : Hardware Asset , “BANK ABC” Assets , PROD Assets]

4.9) Asset Register

The organization authorizes, controls, and **tracks the types of systems** entering and exiting organizational facilities and maintains appropriate records. Use of IT Asset Management tools are highly encouraged to keep track of all Company Assets.

Kindly refer Document ID : SCG/AAR/035/1.0

4.10) Asset Relocation/Transfer

Authorization must be obtained prior to **relocation or transfer** of hardware, software, or data to offsite premises. Assets are prohibited from being removed from [SecureCyberGates] facilities without prior management authorization. Prior to the removal of the system, the following applicable information must be captured:

- Make/model /serial # of the asset
- Owner of the asset
- Reason the asset is being removed from the facility
- Company and name of representative removing the asset
- Estimated return date for asset, if applicable

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

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

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