VENDOR MANAGEMENT POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/VMP/016/1.0
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
SCG/VL/033/1.0			List of Vendors

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 standard operating procedure (SOP) describes the procedures that will be used to onboard vendors/vendor/subcontractors for project work and research activities. These detailed steps promote compliance with [SecureCyberGates] business practices as well as ensuring, as applicable, the vendor/subcontractor complies with regulatory requirements, meets information security standards, and fulfils al ethical responsibilities for protecting the rights and safety of research participants.

While [SecureCyberGates] may transfer any or all the human factors and user experience consulting-related duties and functions to a vendor/subcontractor, the ultimate responsibility for the quality and integrity of the research will always reside with [SecureCyberGates] Therefore, this SOP describes the process for the identification, selection, evaluation, re-evaluation and overall management of vendor/subcontractors and to verify the proposed vendor/subcontractor implements adequate quality assurance and quality control in performing its responsibilities.

2) Roles &Responsibilities

This SOP applies to all research personnel involved in supervising, managing, and conducting research studies as members of [SecureCyberGates], Vendor/subcontractors may only be approved by a director level [Higher Management]; it is their responsibility to assess the suitability and selection of the vendor/subcontractor. As applicable, vendor/subcontractors may be assessed and reviewed with [SecureCyberGates] CISO as well. It is also the responsibility of a Project Lead to manage the vendor/subcontractor to ensure they adequately fulfil their contractual agreement. This responsibility may also be delegated to other research team members with adequate training and knowledge to evaluate/manage the vendor/subcontractor.

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

3) Scope

This SOP applies to all events in which a **vendor/subcontractor** would be used to perform any project related work or Company Operations work with an approved proposal.

4) Process overview

The procedures for Secure Vendor and Third-Party Relationships are essential to ensure that external vendors and third parties, in the event they require access to [SecureCyberGates]'s systems and data, meet the same security standards and expectations as internal stakeholders. This safeguards sensitive information and mitigates potential security risks associated with external relationships.

The process for **selecting, evaluating, re-evaluating and overall managemen**t of a vendor/subcontractor for project work or research activities can be summarized into the follow procedures:

- Define project needs
- Identify potential vendor/subcontractors
- Vendor Assessment and Selection
- Proposal and approval of the vendor/subcontractor
- Vendor Onboarding and Training
- Monitoring and Auditing
- Incident Response and Resolution
- Annual re-evaluation
- Vendor Relationship Termination

5) Procedures

5.1) Define project needs

The Project Lead will work together, as needed, with a Director level [Higher Management] to define project needs which would require the use of a vendor/subcontractor.

The Project Lead and/or a Director level [Higher Management] should obtain approval from the client/sponsor, taking into account any procedures established per a Master Services Agreement, for utilizing vendor/subcontractors.

5.2) Identify potential vendor/subcontractors

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

- The Project Lead or a Director level and above [SecureCyberGates] employee will identify possible vendor/subcontractor service providers.
- The Project Lead or a Higher Management will make initial contact with the potential vendor/subcontractor and request an introductory meeting to discuss the service needs.

5.3) Vendor Assessment and Selection

Vendor Due Diligence

- Prior to onboarding a vendor, due diligence will be conducted to assess their financial stability, reputation, and security track record.
- A vendor risk assessment will help identify potential security risks and assess their impact on [SecureCyberGates] and [SecureCyberGates]'s customers.

Vendor Selection Criteria

- Vendors will be selected based on a combination of factors, including their security practices, compliance with relevant regulations, and alignment with [SecureCyberGates]'s security policies and goals.

5.4) Proposal and approval of the vendor/subcontractor

- [SecureCyberGates] will provide the vendor/subcontractor with an outline of the project, the services required, and any other relevant information (e.g., timeline, budget constraints, technology requirements, etc.) to assist in their development of a formal proposal.

- Prior to the distribution of any confidential information to a vendor/subcontractor, a fuly executed mutual NDA must be obtained.

- [SecureCyberGates] will determine a due date or timeline for which the vendor/subcontractor is obligated to return the formal proposal.

- In their formal proposal, the vendor/subcontractor wil be asked to provide the folowing:
    1. Detailed descriptions as to how they propose to provide services to meet the defined project needs.
    2. An estimate of costs and assumptions associated with the service provision.
    3. Documents that support their qualifications (e.g., quality accreditation/certification, key employees CVs, portfolio samples, capabilities presentations, etc.).

- The Project Lead, in collaboration with the project team members, and Higher Management will review the suitability of the vendor/subcontractor proposal and determine whether to accept or reject the proposal. For the specific project, the vendor/subcontractor should be evaluated on according to:
    1. Ability to fulfill the requirements of the defined project needs
    2. Ability to completed the required activities in the necessary timelines and within the alocated budget

- Security requirements including data protection standards, incident response protocols, and audit rights will be clearly defined in vendor contracts and agreements.

- [SecureCyberGates]'s legal team will review vendor contracts to ensure that they comply with all applicable laws and regulations. Contracts will address data ownership, confidentiality, dispute resolution and handling for security incidents and breaches, including defined escalation paths and incident response expectations.

- Details of all Vendors MUST be maintained in a central tracker **[e.g. Document ID : SCG/VL/033/1.0]**

5.5) Vendor Onboarding and Training

- Vendors who are granted access to [SecureCyberGates]'s systems and data will receive a security orientation, which includes a briefing on security policies, procedures, and access controls. The access granted is only to the specific systems and data necessary for their contracted services and will be tightly controlled and monitored.
- Vendors will be required to undergo ongoing security training and awareness programs. These programs will keep vendors informed about emerging threats and best practices.

5.6) Monitoring and Auditing

Ongoing Monitoring

- Ongoing monitoring of vendor activities will be conducted to ensure compliance with security requirements and contract terms.
- Monitoring tools and techniques will be used for this purpose.

Periodic Audits

- Regular audits of vendor security practices will be performed to verify compliance with security requirements and to assess the overall security posture of the vendor

5.7) Incident Response and Resolution

Incident Reporting

- Vendors will be required to promptly report any security incidents or breaches to [SecureCyberGates].
- Reporting channels and timelines will be defined in vendor contracts.

Incident Coordination

- Procedures for coordinating incident response between [SecureCyberGates] and the vendor will be established.
- This includes predefined responsibilities for each party in the event of an incident.

Resolution and Remediation

- Vendors will be expected to actively participate in incident resolution and remediation efforts.
- Post-incident reviews will be conducted to prevent recurrence.

5.8) Annual re-evaluation

- For a vendor/subcontractor earning an "Accepted Vendor" rating, the vendor/subcontractor will be re-evaluated annually by the Project Manager, CTO, Managers, Operations head. Vendors/subcontractors will be re-evaluated on the following criteria:
  - Quality of product/service
  - Punctuality and response time
  - Cooperation
  - Price
  - Reliability
  - Financial stability

- The following scale will be used to score vendor/subcontractor on the criteria listed above:
  - 5: Excellent- Exceeds expectations/needs
  - 4: Good- meets expectations/needs
  - 3: Acceptable- meets most of our expectations/needs
  - 2: Poor- doesn't reliability meet expectations/needs
  - 1: Very poor- needs major improvement in the short term

- Details of the assessment will be added to the vendor/subcontractor ticket.

- If any "Accepted" vendors/subcontractors are re-evaluated as "Rejected Vendor", the vendor/subcontractor will be notified. And if applicable, given contingencies to implement and improve specific concerns by a certain date.

5.9) Vendor Relationship Termination

Exit Strategy

- Vendor contracts will include an exit strategy to define the termination process and data migration.
- The exit strategy will ensure a smooth transition in the event of contract termination.

Data Ownership

- Ownership of data will be clearly defined in vendor contracts.
- Procedures for data retrieval, destruction, or transfer upon contract termination will be documented.

6) Employee Training and Awareness

6.1) All [SecureCyberGates] employees and Vendors 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 HR department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this 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	HR	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 maintaining the highest standards for Vendor Security and Compliance. Every Vendor/ 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