SOBHAGYA CAPITAL OPTIONS PVT. LTD.
A SEBI Registered Category-1 Merchant Banking Company

CORPORATE OFFICE:-
C-7 & 7A, Gate No. 01, Hosiery Complex, Phase-II Extension
NOIDA – 201 305
Contract- +91 7836066001
E-mail: delhi@sobhagyacap.com
Website: www.sobhagyacapital.com
CIN: U74899DL1994PTC060089
SEBI Regn No. MB/INM000008571

CYBERSECURITY AND CYBER RESILIENCE POLICY

Sobhagya Capital Options Private Limited

Version: 1.0
Effective Date: 21.08.2026
Approved By: Board of Directors
Review Frequency: Annually or as required by applicable laws, SEBI circulars and regulations

I. PURPOSE

The purpose of this Cybersecurity and Cyber Resilience Policy **("Policy")** is to establish a framework governing the cybersecurity and cyber resilience posture of **Sobhagya Capital Options Private Limited ("SCOPL" or "Company"), a SEBI registered Category I Merchant Banker.**

The Policy is intended to:

- safeguard the confidentiality, integrity and availability of the Company's information systems and data;
- protect Unpublished Price Sensitive Information ("UPSI") and other confidential client and deal information from cyber threats;
- ensure compliance with SEBI's Cybersecurity and Cyber Resilience Framework ("CSCRF") and other applicable regulatory requirements;
- establish clear governance, roles and accountability for cybersecurity within the Company;
- enable the Company to anticipate, withstand, contain, recover from and evolve beyond cyber incidents; and
- maintain the trust, integrity and reputation of the Company as a Merchant Banker.

II. APPLICABILITY

This Policy shall apply to:

1. all employees, directors, Designated Person, officers and KMPs of the Company, regardless of location or employment type;
2. all information systems, networks, applications and devices owned, leased or used by the Company in connection with its merchant banking activities;
3. all data, physical or electronic, created, received, stored or transmitted by the Company, including UPSI and deal-related confidential information;
4. third-party vendors, consultants, legal counsel, printers, registrars and other service providers who access, process or store the Company's data or connect to its systems; and
5. any other person or system specifically designated by the Compliance Officer for the purpose of this Policy.

III. REGULATORY FRAMEWORK

This Policy shall be read in conjunction with applicable laws, rules and regulations, including:

- SEBI Circular on the Cybersecurity and Cyber Resilience Framework **(CSCRF)** for SEBI Regulated Entities, and subsequent clarificatory circulars;
- SEBI (Merchant Bankers) Regulations, 1992, as amended;
- SEBI (Prohibition of Insider Trading) Regulations, 2015, to the extent UPSI handling intersects with information security;

Sobhagya Capital Options Pvt. Ltd. New Delhi

- directions issued by the Indian Computer Emergency Response Team **("CERT-In"),** including the CERT-In Cyber Security Audit Policy Guidelines;
- Information Technology Act, 2000, and rules made thereunder;
- applicable provisions of the Companies Act, 2013; and
- any other applicable law, circular, guideline or regulatory direction.

In case of any inconsistency between this Policy and applicable law, the provisions of applicable law shall prevail.

IV. DEFINITIONS

1. **"Critical Systems"**

Critical Systems means systems that are key to business continuity, client-facing applications, and systems connected to the Company's core operational network, including systems used for DRHP drafting and due diligence data rooms.

2. **"Cyber Incident"**

Cyber Incident means any event that actually or potentially jeopardises the confidentiality, integrity or availability of the Company's information systems or data.

3. **"IT Committee"**

IT Committee means a committee for cybersecurity oversight including at least one external, independent cybersecurity expert. Constitution of an IT Committee is not presently mandatory for the Company as a Small-size RE, but shall be required if the Company's CSCRF classification changes, as set out in Clause V of this Policy

4. **"UPSI"**

Unpublished Price Sensitive Information shall have the meaning assigned to it under the SEBI (Prohibition of Insider Trading) Regulations, 2015.

5. **"VAPT"**

VAPT means Vulnerability Assessment and Penetration Testing.

6. **"RE"**

RE means a Regulated Entity as defined under the CSCRF, and includes the Company for the purposes of this Policy.

7. **"Small-size RE"**

Small-size RE means the classification assigned to the Company under the CSCRF's risk-based categorisation of Regulated Entities, determined at the start of each financial year based on the preceding year's data, which determines the scope of CSCRF obligations applicable to the Company.

8. **"Designated Officer"**

Designated Officer means, in accordance with CSCRF **("IT Committee for REs"),** the individual who reviews and approves the Company's CSCRF compliance in the absence of an IT Committee, being the Company's Managing Director, Chief Executive Officer, or a Board Member.

V. CLASSIFICATION UNDER THE CSCRF

The CSCRF adopts a graded, risk-based approach and classifies Regulated Entities into categories — Market Infrastructure Institutions ("MIIs"), Qualified REs, Mid-size REs, Small-size REs, and Self-certification REs — with obligations scaled to each category. The Company is presently classified as a Small-size RE. Accordingly, certain CSCRF obligations that apply only to MIIs, Qualified REs, or Mid-size REs — including mandatory constitution of an IT Committee with an external cybersecurity expert, mandatory ISO/IEC 27001 certification, and Cyber Capability Index assessment — do not presently apply to the Company, and this Policy is drafted accordingly.

The Company's classification shall be reassessed at the start of each financial year in accordance with SEBI's prescribed thresholds. If the Company's classification changes, the Compliance Officer shall promptly review and, where necessary, amend this Policy to bring it into line with the obligations applicable to the revised category, including constituting an IT Committee and/or obtaining ISO/IEC 27001 certification within the timeline prescribed by SEBI.

VI. GOVERNANCE STRUCTURE

The Board of Directors holds ultimate responsibility for the Company's cybersecurity and cyber resilience and shall:

Sobhagya Capital Options Pvt. Ltd. New Delhi

- approve this Policy and any material amendments to it;
- receive a cybersecurity update at least quarterly, covering incidents, audit findings, VAPT results and remediation status; and
- approve and annually review the Company's risk appetite for cyber risk.

Designated Officer (in lieu of an IT Committee — Small-size RE).

In accordance with CSCRF Section 3 ("IT Committee for REs"), in the absence of an IT Committee, CSCRF compliance shall be reviewed and approved by a Designated Officer, being the Company's Managing Director, Chief Executive Officer, or a Board Member. Accordingly:

- the Board shall designate one individual holding the office of Managing Director, Chief Executive Officer, or Board Member as the Designated Officer for the purposes of this Policy;
- the Designated Officer shall review and approve the Company's CSCRF compliance, including this Policy, VAPT and Cyber Audit outcomes, and material cybersecurity decisions;
- the Compliance Officer shall support the Designated Officer by coordinating day-to-day cybersecurity governance, tracking regulatory deadlines, and preparing compliance material for the Designated Officer's review; and
- if the Company's CSCRF classification changes to a category for which an IT Committee is mandatory, the Company shall constitute such a Committee, including an external independent cybersecurity expert, within the timeline prescribed by SEBI.

While it is not mandatory for Small-size REs and Self-certification REs to setup an IT Committee for REs, it is desirable to include and IT expert in decision-making given the ever expanding role of IT in securities market. Therefore, In the absence of IT Committee for REs for Small-size REs and Self certification REs, the compliance to CSCRF shall be reviewed and approved by MD/ CEO/ Board member.

VII. ROLES AND RESPONSIBILITIES

Without prejudice to the generality of Clause V, the following roles and responsibilities shall apply:

- **Board of Directors:** final approval of this Policy, approval of risk appetite, and quarterly review of the Company's cyber posture;
- **IT Committee:** policy oversight, review of VAPT and audit results, and independent expert input;
- **Compliance Officer:** regulatory alignment, SEBI reporting, monitoring adherence to this Policy, and escalation of breaches;
- **Cybersecurity Coordinator:** day-to-day risk management, incident response coordination, and vendor and technical oversight; and
- **All Employees:** adherence to this Policy, prompt reporting of suspected incidents, and completion of mandated training.

VIII. RISK IDENTIFICATION AND ASSET MANAGEMENT

The Company shall maintain a comprehensive and current inventory of its information assets, including hardware, software, applications, data repositories and third-party connections. This inventory shall be reviewed at least annually and updated whenever material changes occur.

The Company shall classify its data based on sensitivity, with particular care given to:

- UPSI relating to client transactions and deals under mandate;
- client financial records and promoter or litigation information gathered during due diligence; and
- internal Company records, including books of account and correspondence with SEBI.

A risk assessment shall be conducted at least annually, mapping identified threats and vulnerabilities to specific Critical Systems and data assets, with results reported to the IT Committee/Designated Officer.

VIII. ACCESS CONTROL

- Access to systems and data shall be granted on a role-based, least-privilege basis.
- Deal team members shall have access only to information relevant to their active mandates; access to closed or unrelated deal files shall be restricted.

- Multi-factor authentication shall be enabled for email, remote access, and any system storing UPSI or client-sensitive data.
- User access rights shall be reviewed periodically and revoked promptly upon change of role or cessation of employment.

IX. DATA PROTECTION

- Sensitive data, including UPSI and due diligence files, shall be encrypted both at rest and in transit.
- Data shall be stored in accordance with applicable data localisation requirements.
- Use of removable media and personal devices for Company data shall be restricted and, where permitted, subject to encryption and prior approval.

X. THIRD-PARTY AND VENDOR RISK MANAGEMENT

- Vendors, legal counsel, printers, registrars and other third parties with access to the Company's data or systems shall be subject to a security due diligence review prior to onboarding.
- Contracts with such third parties shall include confidentiality obligations, security requirements and incident notification clauses.
- A current list of third parties with access to Company systems or data shall be maintained and reviewed periodically.

XI. EMPLOYEE AWARENESS AND TRAINING

- All employees shall undergo cybersecurity awareness training at induction and at least annually thereafter.
- Training shall cover phishing awareness, secure handling of UPSI, password hygiene and incident reporting procedures.
- Periodic simulated phishing exercises shall be conducted.

XII. DETECTION AND MONITORING

The Company shall implement continuous or periodic monitoring of its Critical Systems, appropriate to its size and risk profile, either through an in-house arrangement or an outsourced managed security service. Monitoring shall be designed to generate auditable evidence of detection capability, consistent with CSCRF expectations.

XIII. VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Vulnerability Assessment and Penetration Testing ("VAPT") shall be conducted:

- at the frequency prescribed for the Company's CSCRF category, being at least once, and up to twice, in a financial year;
- following any major system change, upgrade or regulatory change affecting the Company's IT environment; and
- with the VAPT report submitted to SEBI within one month of completion, accompanied by a declaration signed by the Managing Director or Chief Executive Officer.

XIV. CYBER AUDIT

A Cyber Audit shall be conducted at least once, and up to twice, based on the Company's CSCRF category, in each financial year, covering all Critical Systems and a representative sample of non-critical systems. The Cyber Audit report shall be submitted to SEBI within one month of completion.

XV. INCIDENT RESPONSE PLAN

The Company shall maintain a Board-approved Incident Response Plan naming specific owners for detection, containment, communication and recovery. The plan shall be tested periodically through drills or tabletop exercises and updated based on lessons learned.

XVI. INCIDENT REPORTING TO SEBI

Any reportable cyber incident shall be escalated internally to the Cybersecurity Coordinator and Compliance Officer immediately upon detection, and shall be reported externally as follows:

- initial intimation to SEBI at mkt_incidents@sebi.gov.in within six (6) hours of detection;
- a detailed incident report submitted through the SEBI Incident Reporting Portal within twenty-four (24) hours of detection;
- a root cause analysis submitted within the period specified by SEBI following the incident; and
- a quarterly summary report of cyber-attacks, threats, incidents and breaches, submitted to SEBI within fifteen (15) days of the end of each quarter (June, September, December and March).

XVII. BUSINESS CONTINUITY AND DISASTER RECOVERY

- The Company shall maintain a Business Continuity and Disaster Recovery plan defining recovery time objectives for Critical Systems.
- Backups of critical data shall be maintained, tested periodically for restorability, and stored securely, including off-site or in the cloud as appropriate.
- The Business Continuity and Disaster Recovery plan shall be reviewed and tested at least annually.

XVIII. CERTIFICATION REQUIREMENTS

As a Small-size RE, the Company is not presently required to obtain ISO/IEC 27001 certification — such certification being mandatory only for Market Infrastructure Institutions and Qualified REs under the CSCRF. The Company may voluntarily adopt ISO/IEC 27001 as a best-practice benchmark for its information security management systems, and shall obtain and maintain such certification within the timeline prescribed by SEBI if the Company's classification changes to a category for which certification is mandatory.

XIX. RECORD KEEPING

The Company shall maintain records relating to:

- asset inventories and risk assessments;
- VAPT and Cyber Audit reports and related declarations;
- cyber incidents, root cause analyses and remediation actions;
- Board minutes relating to cybersecurity; and
- any other records required under applicable law.

Records shall be maintained for the period prescribed under applicable regulations.

XX. CONTINUOUS IMPROVEMENT

Following any cyber incident, audit or VAPT exercise, the Company shall conduct a lessons-learned review and update this Policy, its controls and its Incident Response Plan accordingly. The Company shall stay informed of emerging threats and evolving SEBI and CERT-In requirements through regular monitoring of regulatory circulars and industry advisories.

XXI. VIOLATION OF POLICY

Any violation of this Policy may result in appropriate disciplinary action in accordance with the Company's internal procedures. Depending upon the nature and severity of the violation, disciplinary action may include:

- written warning;
- restriction or suspension of system access;
- monetary penalty, where permissible;
- suspension from employment;
- termination of employment; and/or
- reporting to the appropriate regulatory authority.

Regulatory or statutory penalties, where applicable, shall be in addition to internal disciplinary action.

XXII. DUTY TO REPORT

Any employee who becomes aware of a suspected cyber incident, breach of this Policy, or unauthorized access to or disclosure of the Company's systems or data, shall promptly report the matter to the Compliance Officer or the Cybersecurity Coordinator. No employee shall suffer retaliation for making a bona fide report under this Policy.

XXIII. REVIEW OF POLICY

This Policy shall be reviewed at least annually by the "Designated Officer" and placed before the Board for re-approval, or earlier if triggered by a material cyber incident, a significant change in the Company's IT environment, or an update to applicable SEBI or CERT-In requirements.

XXIV. BOARD APPROVAL

This Policy has been approved by the Board of Directors of **Sobhagya Capital Options Private Limited** and shall be effective from the date specified above.

For Subhagya Capital Options Private Limited

SHWETA JAIN
Digitally signed by SHWETA JAIN
Date: 2026.08.26 12:17:41 +05'30'

Authorized Signatory / Compliance Officer
Date: 21.08.2026