Ref. No. OPC/2024-25/Legal/104 **Date**: 01 June, 2024

Cybersecurity Policy

1. Purpose

The purpose of this Cybersecurity Policy ("Policy") is to protect the information and technology assets of HedgeMyFunds ("Company") from all forms of cyber threats, ensuring the confidentiality, integrity, and availability of data and systems.

2. Scope

This Policy applies to all employees, contractors, consultants, temporary staff, and other workers at the Company, including all personnel affiliated with third parties. It covers all data, systems, networks, devices, and applications owned or managed by the Company.

3. Roles and Responsibilities

3.1 Board of Directors

- Provide oversight and ensure the effectiveness of the cybersecurity program.
- Approve the Cybersecurity Policy and any significant changes to it.
- Review regular cybersecurity reports.

3.2 Chief Information Security Officer (CISO)

- Develop, implement, and maintain the cybersecurity program.
- Monitor the effectiveness of cybersecurity measures and report to the Board of Directors.
- Ensure compliance with cybersecurity regulations and best practices.

3.3 IT Department

- Implement technical controls to protect the Company's information systems.
- Monitor and respond to security incidents and vulnerabilities.
- Conduct regular security assessments and audits.

3.4 Employees

- Adhere to the cybersecurity guidelines and procedures outlined in this Policy.
- Report any suspicious activities or security incidents to the IT Department immediately.
- Participate in cybersecurity training and awareness programs.

Ref. No. OPC/2024-25/Legal/104 **Date**: 01 June, 2024

4. Cybersecurity Principles

4.1 Confidentiality

- Ensure that sensitive information is accessible only to those authorized to access it.
- Implement data classification and access control measures.

4.2 Integrity

- Protect data from unauthorized modification or destruction.
- Utilize checksums, hashes, and encryption to ensure data integrity.

4.3 Availability

- Ensure that information and systems are available to authorized users when needed.
- Implement redundancy and disaster recovery plans.

5. Security Controls

5.1 Access Control

- Implement role-based access control (RBAC) to limit access to information and systems based on job responsibilities.
- Use multi-factor authentication (MFA) for accessing sensitive systems.

5.2 Data Protection

- Encrypt sensitive data both in transit and at rest.
- Regularly back up data and store backups securely.

5.3 Network Security

- Use firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways to protect the Company's network.
- Segment the network to isolate critical systems and sensitive data.

5.4 Endpoint Security

- Ensure all endpoints (computers, mobile devices, etc.) have up-to-date antivirus and anti-malware protection.
- Implement device management policies to control the use of personal devices.

Ref. No. OPC/2024-25/Legal/104 **Date**: 01 June, 2024

5.5 Incident Response

- Develop and maintain an incident response plan to address and manage security incidents.
- Conduct regular incident response drills and training sessions.

5.6 Training and Awareness

- Provide ongoing cybersecurity training and awareness programs for all employees.
- Conduct phishing simulations and other exercises to test employee readiness.

6. Compliance and Legal Requirements

- Ensure compliance with all relevant laws, regulations, and industry standards related to cybersecurity.
- Conduct regular audits to verify compliance and address any deficiencies.

7. Monitoring and Reporting

- Continuously monitor the Company's networks and systems for signs of cyber threats.
- Report security incidents and breaches to the appropriate authorities as required by law.
- Provide regular cybersecurity reports to senior management and the Board of Directors.

8. Review and Update

This Policy will be reviewed annually or more frequently as needed to ensure its continued relevance and effectiveness. Any significant changes to the Policy will be approved by the Board of Directors.

9. Policy Enforcement

Compliance with this Policy is mandatory. Violations may result in disciplinary action, up to and including termination of employment. The Company reserves the right to take legal action in cases of serious breaches.

10. Contact Information

For any questions or concerns regarding this Policy, employees should contact the IT Department or the CISO at:

it@hedgemyfunds.co.in
+91 98883 34677

Effective Date: 3 June, 2024

Ref. No. OPC/2024-25/Legal/104 **Date**: 01 June, 2024

Acknowledgment of Receipt and Understanding

I, [Employee Name], have read and understand the Cybersecurity Policy of HedgeMyFunds. I agree to adhere to the guidelines and expectations outlined in this Policy.

_____
[Employee Name]
[Employee Signature]
[Date]

_____
[Supervisor Name]
[Supervisor Signature]
[Date]