Policy on Cyber Security and Cyber Resilience

Introduction

We, **Wealthstreet Financial Services Private Limited** (the "Company"), are a financial services provider offering brokerage and investment-related services. As we handle sensitive client information and participate in the securities market, maintaining a robust **Cyber Security** and **Cyber Resilience** framework is critical to protect data and ensure the continuous operation of our services, especially in the event of cyber-attacks.

This **Cyber Security and Cyber Resilience Policy** was adopted by the Company's Board and is effective from **April 1, 2019** to comply with SEBI's Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated **December 03, 2018** on cyber security and resilience requirements for market participants.

Background

With rapid technological advancements, the risk of cyber-attacks in the securities market has significantly increased. **Wealthstreet Financial Services Private Limited** recognizes the importance of adapting a security framework to protect our IT assets, client data, and network systems from potential breaches. Our Cyber Security policy aims to ensure that we manage, monitor, and mitigate risks associated with our operations in compliance with applicable guidelines.

Cyber Security and Cyber Resilience Objectives

The **Cyber Security** framework ensures the **Confidentiality**, **Integrity**, and **Availability (CIA)** of our critical systems and data:

- **Confidentiality**: Limiting access to systems and information to authorized users.
- **Integrity**: Ensuring that the information is reliable, accurate, and tamper-free.
- **Availability**: Guaranteeing that systems and data are accessible to authorized users when needed.

Cyber Resilience refers to the ability to respond to, recover from, and continue operations despite cyber-attacks or data breaches.

Governance Structure

1. **Risk Management Framework**: We have implemented a comprehensive risk management framework to address the cyber threats to our systems, networks, and databases. The policy follows the guidelines set out in international best practices such as **ISO 27001** and **COBIT 5**.
2. **Designated Cyber Security Officer**: Mr. **Mitul Gandhi**, CISO (Chief Information Security Officer) of the Company, is responsible for overseeing cyber security risk assessment, incident response, and the establishment of appropriate controls and procedures to mitigate risks.

3. **Regular Reviews and Reporting**: The **Cyber Security Team** will periodically assess cyber threats domestically and globally. They will take proactive steps to ensure continuous improvement in our security framework.

Identification of Cyber Risks

- **Critical Assets Identification**: The Company identifies sensitive business operations, data management, and IT systems as critical assets. These are evaluated to determine the risks and impact of potential cyber threats.
- **Up-to-Date Asset Inventory**: The Company maintains an updated inventory of hardware, software, systems, and personnel involved in the management of IT assets.

Cyber Security Measures

1. **Access Controls**: Access to critical systems, applications, and networks will be granted on a "need-to-use" basis. The principle of **least privilege** will be applied to minimize risks. We will ensure that access control policies address strong password requirements and restrict unnecessary access to systems.
2. **Physical Security**: Physical access to critical systems will be restricted to authorized personnel. Outsourced staff or visitors will be monitored and escorted during their presence. Office premises will be secured and monitored by security personnel.
3. **Network Security Management**: The Company will establish **baseline security configurations** for all operating systems, network devices, and mobile enterprise devices. Adequate controls will be deployed to prevent attacks such as **viruses**, **malware**, and **ransomware**.
4. **Data Security**: Strong **encryption** methods will be used to ensure data confidentiality during transmission and storage. The Company will also implement security policies on the use of mobile devices and other office equipment.
5. **Application Security**: Security measures will be applied to **customer-facing applications**, especially those exposed to the internet (e.g., **internet-based trading** platforms), to mitigate risks associated with large attack surfaces.
6. **Patch Management**: A systematic approach will be used to identify, categorize, and prioritize software patches and updates. Regular testing will ensure that updates are applied without affecting system functionality.

Disposal of Data and Systems

- The Company will follow a strict **data disposal policy** to ensure that critical information is securely removed from storage devices. Techniques such as **crypto-shredding**, **degaussing**, or **physical destruction** will be used for the disposal of sensitive data and hardware.

Vulnerability Assessment and Penetration Testing (VAPT)

- The Company will regularly conduct **vulnerability assessments** and **penetration tests** to identify and address any potential security vulnerabilities. These tests will be performed annually and prior to the launch of any new publicly accessible systems.

Monitoring and Detection

1. **Security Monitoring**: We will establish systems to continuously monitor security events and logs. These will help in the early detection of unauthorized activities, changes, or breaches in our systems.
2. **Anomaly Detection**: Logs and alerts will be monitored to detect anomalies. Mechanisms like **firewalls** will be used to monitor bandwidth usage, ensuring that unusual traffic patterns are flagged.

Incident Response and Recovery

1. **Incident Management**: In the event of a cyber-attack, we will investigate and mitigate the effect of the incident by executing pre-defined response plans. These plans aim to prevent the spread of the attack and contain the breach.
2. **Recovery**: Our **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)** will comply with SEBI's guidelines as per the **SEBI Circular CIR/MRD/DMS/17/2012**. We will restore operations swiftly to minimize any disruption to services.

Information Sharing and Collaboration

- **Quarterly Reports**: Reports on cyber-attacks, threats, and the measures taken to address them will be shared with other stakeholders, including **Stock Exchanges** and **Depositories**. These reports will provide insight into vulnerabilities and security measures.

Training and Awareness

1. **Employee Training**: We will regularly conduct training programs for all employees, educating them on **cyber threats**, **security protocols**, and the company's **Cyber Security Policy**. These programs will be updated regularly to stay aligned with current threat landscapes.
2. **Third-Party Vendor Compliance**: We will ensure that our third-party vendors and service providers adhere to our **Cyber Security** and **Cyber Resilience** policies by obtaining necessary certifications and audits.

Periodic Audits

- **Annual Audit**: We will conduct an annual audit of our systems by a **CERT-IN** empanelled auditor or a qualified **CISA**/ **CISM** auditor. The audit results will be submitted to the relevant authorities within three months of the end of each financial year.

Conclusion

At **Wealthstreet Financial Services Private Limited**, we are committed to ensuring the security and resilience of our systems. Our **Cyber Security** and **Cyber Resilience** policy aims to protect our clients, employees, and stakeholders from potential cyber risks while ensuring compliance with industry standards and regulations.