Shri Parasram Holdings Pvt Ltd.

Cyber Security & Cyber Resilience Policy

This Policy document is asset of Shri Parasram Holdings Pvt Ltd.

For & exclusive use of

Shri Parasram Holdings Pvt Ltd. (“hereinafter referred as ‘SPHPL').

Owner	**Prepared By -**	**Approved By -**	**Version No.**	**Issue Date**	**Review Date**
Compliance and I.T Department	Compliance Officer	Board of Directors	Version 1	1st April 2019	

Table of Contents

CYBER SECURITY AND CYBER RESILIENCE POLICY

Preface:

- Rapid technological development in securities market have highlighted the need for maintaining robust cyber security and cyber resilience framework to protect the integrity of data and guard against breaches of privacy.
- Since the company performs significant functions in providing services to the holders of securities it is desirable to have a robust cyber security and cyber resilience framework in order to provide essential facilities and perform systematically critical functions relating to securities market.
- Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases. Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

1. Governance

- In order to manage risk to systems, networks and databases from cyber-attacks and threats, SPHPL has formulated this comprehensive Cyber Security and Cyber Resilience Policy ("hereinafter referred as 'Policy') encompassing the framework. The policy document post approval by the Board be reviewed annually to strengthen and improve its Cyber Security and Cyber Resilience framework.

- The Cyber Resilience framework comprises of the following:

a. Identification of critical IT assets and risks associated with such assets:

A list of critical IT assets identified has been listed out in Annexure 1.

Risks/ Threats associated with these assets are Data loss, **malware**, **ransomware**, unauthorized access, Loss of confidentiality etc. Indirect effects include monetary loss associated with the risks/ threats and critical impact on the operations and business of the Company.

An up-to-date inventory of the hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network, resources, connections to its network and data flows shall be maintained.

b. 'Protection of the assets by deploying suitable controls, tools and measures:

This has been covered under the heading 'Network Security Management' in this policy.

c. Detect' incidents, anomalies and attacks through appropriate monitoring tools/ processes

d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.

e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.

- SPHPL shall abide, so far as practical and applicable, to the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of NationalCritical Information Infrastructure') and subsequent revisions, if any, from time to time

- **Appointment of 'Designated Officer':**

  Mr. Anshu Aggarwal (Director)would be the Designated Officer for the purpose of this policy. Functions of the Designated Officer would be to assess identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.

- The Board of the Company shall constitute a Technology Committee to be referred as **'SPHPL Technology Committee'** who would review the implementation of the policy on a half yearly basis. The review would include review of the current IT and Cyber Security and Cyber Resilience capabilities, setting goals for a target level of Cyber Resilience, and establish plans to improve and strengthen Cyber Security and Cyber Resilience, the same shall be placed before the Board for appropriate action. The members of the Committee are listed out in Annexure 2.

- **Reporting procedure to facilitate communication of unusual activities and events to the Designated Officer:**

  All Employees or any other entities who may have privileged access or use systems / networks of company shall have direct access to the Designated Officer through his email id: anshu@sphpl.com to report or highlight any actual or apprehended threats, vulnerabilities, risks to the I.T assets that they may come across.

- The **Designated officer** and the **SPHPL's Technology Committee** will review instances of cyber-attacks, and take steps to strengthen Cyber Security and cyber resilience framework.

2. Protection

- **Access controls**

  a) No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities.
  b) Any access to systems, applications, networks, databases is for a defined purpose and period.
  c) SPHPL has in place an access policy which addresses strong password controls for users' access to systems.
  d) All critical systems accessible over the internet have a two-factor security (such as VPNs, Firewall controls etc.)
  e) Records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs are maintained and stored in a secure location for a time period not less than two (2) years.
  f) SPHPL has deployed controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to critical systems.
  g) Employees and outsourced staff who may be given authorized access to the critical systems, networks and other computer resources are subject to stringent supervision, monitoring and access restrictions.
  h) SPHPL has formulated an Internet access policy to monitor and regulate the use of internet and internet based services like social media sites, internet storage sites within the IT Infrastructure.

i) Access of privileges to users who are leaving the organization are withdrawn promptly.

- **Physical Security**

a) Physical access to authorized officials over critical systems is restricted to minimum and to outsourced staff/visitors is properly supervised.
b) Team at SPHPL ensures that the perimeter of the critical equipments are physically secured and monitored by employing physical human and procedural controls such as the use of CCTVs, card access systems, mantraps, bollards, etc.

- **Network Security Management**

a) SPHPL has established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment.
b) SPHPL has installed network security devices, such as firewalls to protect its IT infrastructure. Adequate controls are deployed to address virus / malware / ransomware attacks.
c) Adequate control measures like antivirus and anti-malware software are deployed to address virus attacks.

- **Data Security**

a) Critical data is identified and encrypted in motion and at rest by using strong encryption methods.
b) Access to SFTP folders and other folders dealing with client data is provided only in case where exceptional approval of supervisors is provided in order to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity-
c) The information security policy also covers use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data and should allow only authorized data storage devices through appropriate validation processes.

d) SPHPL has following in place for Data Security on Customer Facing Applications:

- different kinds of sensitive data shown to the Customer on the frontend application are analyzed to ensure that only what is deemed absolutely necessary is transmitted and displayed;
- Masking portions of sensitive data wherever possible;
- Analysis of data and databases holistically so that different kinds of data can be isolated and cordoned off;
- When an Application transmitting sensitive data communicates over the Internet with the DP / Stock Broking systems of SPHPL, it IS over a secure, encrypted channel to prevent Man-In-The-Middle (MITM) attacks;
- For Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured SSL certificate on the web server is ensured;
- Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

- **Handling of hardware and software**

a) SPHPL has deployed hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
b) Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data are blocked and measures are taken to secure them.

- **Application security in customer facing Applications**

a) SPHPL has in place appropriate measures in relation to Application security for Customer facing applications offered over the Internet (portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by Brokers to Customers) which are listed out below:

- Any Application offered by SPHPL to Customers containing sensitive, private or critical data such as SWSTs, Back office etc. (referred to as “Application” hereafter) over the Internet shall be password protected

with reasonable minimum length. Attempts shall be made to educate Customers of these best practices.

- Passwords, security PINs etc. shall never be stored in plain text and shall be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. One-way cryptographic hashes shall ensure that stored password hashes are never transformed into the original plaintext values under any circumstances.
- After a reasonable number of failed login attempts into Applications, the Customer's account can be set to a "locked" state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation. A cryptographically secure unique link that is sent to the Customer's registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer's registered mobile number, or manually by SPHPL after verification of the Customer's identity etc.
- Customers are reminded within reasonable intervals to update their password and multi-factor credentials and to ensure that their out-of-band authentication reset information (such as e-mail and phone number) are up-to-date.

- Both successful and failed login attempts against a Customer's account are logged for a reasonable period of time. After successive login failures, measures such as After successive login failures, measures such as temporary locking of the account is done which is unlocked by putting a request to customer support from client. Further, the request is captured on the recorded line.

- **Patch management**

a) Patch management procedures include the identification, categorization and prioritization of patches and updates, rigorous testing of security patches and updates is performed before deployment into the production environment. Patch management is done every month.

- **Disposal of data, Systems and storage devices**

    a) A suitable policy is framed for disposal of storage media and systems. The critical data / Information on such devices and systems is removed by using methods such as crypto shredding / degauss / Physical destruction.
    b) Data-disposal and data-retention policy has been formulated to identify the value and lifetime.

- **Vulnerability Assessment and Penetration Testing (VAPT)**

    a) SPHPL shall regularly conduct vulnerability assessment to detect security vulnerabilities in its IT environments exposed to the internet, where systems publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture.

    b) In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empaneled vendors would be reported to the vendors and the exchanges. Remedial actions to be taken to address gaps that are identified.

3. Monitoring and Detection

- Appropriate security monitoring systems and processes are established to facilitate continuous monitoring of security events / alerts for timely detection of malicious activities unauthorized.
- Suitable mechanisms are implemented to monitor capacity utilization of critical systems and networks that are exposed to the internet.

4. Response and Recovery

- Appropriate investigation of Alerts generated from monitoring and detection systems is done.
- SPHPL has established suitable plans for timely restoration of systems affected by incidents of cyber-attacks or breaches and also conducts suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan.

5. Sharing of Information

- Quarterly reports containing information on cyber-attacks and threats experienced and measures taken to mitigate vulnerabilities threats and attacks, If any is submitted to Stock Exchanges and Depositories.

6. Training and Education

- Periodic training programs would be conducted to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts.

7. Systems managed by MIIs

- Where applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for e.g.: NSDL's Speed-e, CDSL's Easiest,NSE's NOW, BSE's BOLT etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs.

****

ANNEXURE 1

LIST OF CRITICAL I.T ASSETS

This Annexure will be intentionally left blank in the web version of the policy for protecting the confidentiality of the I.T assets.

ANNEXURE 2

MEMBERS OF THE TECHNOLOGY COMMITTEE

Mr. Anshu Aggarwal	Designated Officer, Head of the Committee
Mr. Vivek Sheel Aggarwal	Member
Mr. Prakash Upreti	Member
Mr.Rakesh Kumar Singh	Member
Mr.Sambhav Aggarwal	Member