PCMPL
Parwati Capital Market
Private Limited

CYBER SECURITY POLICY

(Parwati Capital Market Pvt Ltd)
(Version 1.5)

PARWATI CAPITAL MARKET PVT. LTD., herewith referred as <PCMPL>, is the SEBI registered Stock Broker & Depository Participant. The under-mentioned cyber security and cyber resilience policy is created by the Compliance Officer and approved by the Board of Directors on 17.05.2019.

This Sample Cyber Security Policy applies to all employees of Parwati Capital Market Pvt Ltd who have access to computers and the Internet to be used in the performance of their work. Use of the IT of the company is permitted for the employees where such use supports the goals and objectives of the business. However, access to the IT infrastructure of the company is a privilege and all employees must adhere to the policies concerning Computer, Email and Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment.

Employees may also be held personally liable for damages caused by any violations of this policy. All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

If an employee is unsure about what constituted acceptable Compute/Internet usage, then he/she should ask his/her supervisor for further guidance and clarification

All terms and conditions as stated in this document are applicable to all users of company's network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by the company.

WATI CAPITAL MARKET
KOLKATA

Raghav Bagri

1. STATUTORY MANDATE

This framework is formed in accordance with the requirements of the SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 ("the circular") dated December 3, 2018.

SEBI has issued circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019,SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022,SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 and SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023 providing guidelines on Cyber Security and Cyber Resilience. The objectives of the said circulars are to adapt to the rapid technological developments in Securities Market which have highlighted the need for robust Cyber and Cyber Resilience at the level of Stock Brokers/Depository Participants who are performing significant functions in providing services to the holder of Securities.

1) OBJECTIVE OF THE FRAMEWORK

The objective of this framework is to provide robust cyber security and cyber resilience to the Stock brokers and depository participants to perform their significant functions in providing services to the holders of securities.

2) APPLICABILITY

Provisions of the said circular and framing of cyber security and cyber resilience are required to be complied by all Stock Brokers and Depository Participants registered with SEBI. The policy has been reviewed, taken on record and approved by the board of directors of the company at their duly convened meeting held on **06.06.2024.**

3) Cyber Security and Cyber Resilience Policy document.

Cyber-attacks and threats attempt to compromise the confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information's to authorized users only, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). 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 with ease, and to recover from it. With the view to strengthen and improve the Cyber Security and Cyber Resilience framework, the Board of Directors shall review the policy and its implementation, once annually at least.

4) CISO (Chief Information Security Officer)

The **CISO (Chief Information Security Officer)** As per NSE Circular No: NSE/INSP/5224 The Company naominates Mr. Karana Kant Damani as the Chief Information Security Officer of the Company with

PARWATI CAPITAL MARKET PVT. LTD. KOLKATA effect from 01.06.2022, who will be responsible for developing and implementing an information security policy , which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats. The CISO directs the staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information technology (IT) risks.

If any incident occurs immediate reporting of Incident to CERT-IN by CISO and in his absence by the DO or MITC. In case the incident is not reported to CERT-IN, proper documented reason to be kept in record.

Roles & Responsibilities of CISO

Implementing and overseeing our organisation's cyber security program:
A key responsibility for **CISO** within our organisation is to provide guidance on our cyber security program on a strategic level. Along with guidance, it is CISO's responsibility to make sure organisations remain compliant with cyber security standards, policy, regulations and legislation.

Reporting on cyber security:
CISO play an important role when it comes to providing business leaders with intelligence on key cyber security trends. For example, providing the board of directors or senior executives with information like; the security risk profile of the organisation, any cyber security improvements in motion, notable cyber security incidents the return on investment on past cyber security initiatives. It is vital that CISO provide upper-level management with a consolidated and comprehensive view of their organisation's cyber security posture.

5) DESIGNATED OFFICER

The Company nominates Chandra Prakash Srivastava as the Designated Officer of the company to access, identify, and reduce security and Cyber security risks. He is responsible to respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedure as per the Cyber Security Policy.

Designated Officer of the company to assess, identify, and reduce security and Cyber Security risks, r espond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.

6) CONSTITUTION OF TECHNOLOGY COMMITTEE

a) The company constitutes a technology committee ("the committee") with following members:

Sr. No.	Name of the Committee Member	Designation
1	Soumyadipto Ghosh	IT Engineer
2	Shatrughan Sharma	IT Engineer

PARWATI CAPITAL MARKETS * LTD.
KOLKATA

b) Such committee shall on an yearly basis review the implementation of the Cyber Security and Cy ber Resilience policy. Such review shall include but not limited upto, reviewing of current IT and Cyber Security and Cyber Resilience capabilities, setting up of goals for a target level of Cyber Resilience, and establishing plans to improve and strengthen Cyber Security and C yber Resilience. The review shall be placed before the Board of directors for taking appro priate action(s), if required.

c) The Designated officer and the technology committee shall periodically review instances ofcyber attacks, if any, and take steps to strengthen Cyber Security and Cyber Resilience framework.

7) IDENTIFICATION, ASSESSMENT AND MANAGEMENT OF CYBER SECURITY RISK

The company shall ensure the following steps in order to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems.

a) IDENTIFICATION OF CRITICAL IT ASSETS AND RISKS ASSOCIATED WITH SUCH ASSETS

The committee and designated officer shall identify the critical assets based on their sensitivity and criticality for business operations, services and data management including various servers, data processing systems, and information technology (IT) related hardware and software etc.

The IT team shall maintain up-to-date inventory of its 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.

8) ACCEPTABLE USAGE POLICY.

Computer Access Control – Individual's Responsibility

Access to the company's IT systems and trading software's are controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the company's IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any company's IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access company's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to the company's IT systems or information.
- Attempt to access data that they are not authorized to use or access.

PARWATI CAPITAL MARKET PVT. LTD. * KOLKATA

- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non-company's authorized device to the company's network or IT systems.
- Store company's data on any non-authorized company's equipment.
- Give or transfer company's data or software to any person or organization, without the authority of company's IT department.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, company's enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with company's remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smart phones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only company's authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that are authorized by the company on company's laptop/computers. Authorized software must be used in accordance with the software supplier's

PARWATI CAPITAL MARKET PVT. LTD.
KOLKATA

licensing agreements. All software on company's computers must be approved and installed by the company's IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on company's IT equipment.

Viruses

The IT department has implemented centralized, automated virus detection and virus software updates within the company. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved company's anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of the company's voice equipment is intended for business use. Individuals must not use the company's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

- Use (Acme Corporation's) voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

Actions upon Termination of Contract

All company's equipment and data, for example laptops and mobile devices including telephones, smart phones, USB memory devices and CDs/DVDs, must be returned to the company at termination of contract.

All the company's data or intellectual property developed or gained during the period of employment remains the property of the company and must not be retained beyond termination or reused for any other purpose.

PARWATI CAPITAL MARKET PVT. LTD.
KOLKATA

Monitoring and Filtering

All data that is created and stored on the company's computers is the property of the company and there is no official provision for individual data privacy, however wherever possible the company will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Company has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

9) E-WASTE POLICY.

We at the company try to reduce the amount of e-waste created. But upon the end of the life of electronic systems, they need to be disposed off and replaced. Therefore at the time of disposing off the system, the data on the system is securely deleted and removed, such that it is not possible to be reconstructed.

10) DEFINE SUPPLIER RELATIONSHIP MANAGEMENT POLICY.

Whenever the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of the company are managed by vendors and the company may not be able to implement some of the aforementioned guidelines directly, the company shall, from time to time, instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

11) RESPONSIBILITIES OF EMPLOYEES, MEMBERS AND PARTICIPANTS

In addition to the followings, the employees, members and participants shall be responsible for the duties and obligations as may be entrusted and communicated by the company / committee / designated officer from time to time.

To prevent the cyber attacks, the employees, members and participants shall assist the company to mitigate cyber attacks by adhering the followings:

- No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities.
- To attend the cyber safety and trainings programs as conducted by the company from time to time.
- To endure installation, usage and regular update of antivirus and antispyware software on computer used by them.
- Use a firewall for your Internet connection.
- Download and install software updates for your operating systems and applications as they become available.

PARWATI CAPITAL MARKET PVT. LTD.
KOLKATA

- Make backup copies of important business data and information. (Annexure A)
- Control physical access to your computers and network components. (Annexure B)
- Keep your Wi-Fi network secured and hidden.
- To adhere limited employee access to data and information and limited authority to install software.
- Regularly change passwords. (Annexure B)
- Do not use or attach unauthorized devices.
- Do not try to open restricted domains.
- Avoid saving your personal information on computer or any financial data on any unaut hentic website.
- To get your computer regularly scanned with anti-virus software.
- Do not release sensitive data of the organization.

12) REPORTING PROCEDURE TO COMMUNICATE THE UNUSUAL ACTIVITIES AND EVENTS

This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network. Some examples of security incidents are:

a) Illegal access of a company computer system. For example, a hacker logs onto a production server and copies the password file.

b) Damage to a company computer system or network caused by illegal access. Releasing a virus or worm would be an example.

c) Denial of service attack against a company web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.

d) Malicious use of system resources to launch an attack against other computer outside of the company network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their (Designated Officer) immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem. The incident should be reported at the earliest, so that corrective measures shall be taken fast. Upon receiving the report, the committee would look into the matter and take the corrective measures.

13) BUSINESS CONTINUITY

In an event of an attack or network failure, we have the following provisions in place to provide access:

a) Having provision of 3 different point-to-point connection, for easy switchover of network incase theirs connectivity issues in one line.
b) Branch office having all the requirements to act as a backup in case, connecting through main office is not possible.

14) PASSWORD POLICY.

User passwords should remain confidential and not be shared, posted or otherwise divulged in any manner. Company will follow the password guidelines given below. If systems do not support these settings an exception must be filed to that effect.

a) General
   i) All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
   ii) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every quarter.
   iii) Passwords shall not be placed in emails unless they have been encrypted / the network traffic is encrypted.

b) Trading Application Password
   i) The Password is masked at the time of entry.
   ii) System mandated changing of password when the user logons for the first time.
   iii) Automatic disablement of password on entering erroneous password on three consecutive occasions.
   iv) Password shall be alphanumeric and neither only alpha nor only numeric.
   v) Password shall be changed at an interval of fourteen calendar days.
   vi) Password shall not be same as last eight passwords.
   vii) Password shall not be same as User Login ID.
   viii) Password shall be encrypted in the database so that it cannot be viewed by any one at any point of time.
   ix) The session shall be reinitialized upon modification of password by the user.

15) LOG-ON PROCEDURE

Logging onto the trading platform, servers, and computers are protected. Only authorized persons are allowed to log in. With each system having a unique user name and password combination, which is not be disclosed.

16) Log management and monitoring policy.

Trading software's & servers used to implement trades in the market all produce logs. These logs mention all details with respect to the trades executed, orders executed, cancelled and many other details. Therefore it is very important to store these logs daily. Daily logs of the server need to be backed up. The logs are stored onto an external device. Automatic daily backup time should be fixed in the server. Once the external storage device is full, the device should be changed.

17) Illustrative Measures for Backup & Restoration of Data

Back- up is an important aspect of computer data security and all the important data holding servers of the company are to be backed up (W.R.T the Asset Inventory List). Servers expected to be backed up include the database server, the trading - application server, the mail server, and the file server.

Back Up procedure will be as follows:

i) The IT Department will be responsible for daily backup of the files onto an external device or in the cloud.

ii) Three different external storage device should be maintained to backup of data, with 1 taking back up daily, whereas the 2nd for taking weekly back up and the 3rd for monthly backups.

iii) All three devices shall be stored at three different location, to attain extra security.

iv) Every 1st Saturday of the month, the data from the device storing daily back up should be restored and checked. Whereas the other devices shall be restored every quarter to check for any loss of data.

18) Define Internet Access Policy for Internet and internet-based services.

a) Computer, email and internet usage

i) Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted

ii) Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role

iii) All Internet data that is composed, transmitted and/or received by <company's> computer systems is considered to belong to <company> and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties

iv) The equipment, services and technology used to access the Internet are the property of <company> and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections

v) Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images

PARWATI CAPITAL MARKET PVT. LTD.
KOLKATA

vi) All sites and downloads may be monitored and/or blocked by <company> if they are deemed to be harmful and/or not productive to business

vii) The installation of software such as instant messaging technology is strictly prohibited

b) Unacceptable use of the internet by employees includes, but is not limited to:

i) Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via company's email service

ii) Using computers to perpetrate any form of fraud, and/or software, film or music piracy

iii) Stealing, using, or disclosing someone else's password without authorization

iv) Downloading, copying or pirating software and electronic files that are copyrighted or without authorization

v) Sharing confidential material, trade secrets, or proprietary information outside of the organization

vi) Hacking into unauthorized websites

vii) Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers

viii) Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems

ix) Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities

x) Passing off personal views as representing those of the organization

19) Critical system, network and other computer resources user access provisioning and information access restriction for employees.

Access to critical systems and networks is restricted. Only authorized persons are allowed to access it. The systems are password protected with unique user id to access. If any third party is given access it is under the supervision of an authorized person. The server room is under CCTV surveillance and all activities done inside are monitored.

20) Visitor Management.

Visitor register is to be maintained. The register would be placed at the entrance, at time of entering the visitor will require to fill up the register. Namely the details required in the register would be name, address, mobile number, person to meet, and purpose of visit.

21) Access control policy for secure LAN and wireless networks.

The LAN and wireless network shall be password protected. The network shall only be accessed by the people authorised to access them. The password shall be changed on a regular basis so that no

PARWATI CAPITAL MARKET PVT. LTD.
KOLKATA

one is able to access the network.

22) Hardening policy.

Hardening is the process of securing a system by reducing its surface of vulnerability. By the nature of operation, the more functions a system performs, the larger the vulnerability surface.

Most systems perform a limited number of functions. It is possible to reduce the number of possible vectors of attack by the removal of any software, user accounts or services that are not related and required by the planned system functions. System hardening is a vendor specific process, as different system vendors install different elements in the default install process.

Without effective hardening there is an increased risk of the unavailability of systems. This can be caused by attackers, viruses and malware exploiting systems. If external systems such as web servers and email servers advertise their type and version, it makes it easier for an attacker to exploit known weaknesses.

Systems which run unnecessary services and have ports open which do not need to be open are easier to attack as the services and ports offer opportunities for attack.

All new systems will undergo the following hardening process.

i) System Installation

   The system should be installed as per vendors instructions

ii) Remove Unnecessary Software

   Most some systems come with a variety of software packages to provide functionality to all users. Software that that is not going to be used in a particular installation should be removed or uninstalled from the system.

iii) Disable or Remove Unnecessary Usernames

   Most systems come with a set of predefined user accounts. These accounts are provided to enable a variety of functions. Accounts relating to services or functions which are not used should be removed or disabled. For all accounts which are used the default passwords should be changed. Consideration should be given to renaming predefined accounts if it will not adversely affect the system.

iv) Disable or remove Unnecessary Services

   All services which are not going to be use, should be removed from the systems

v) Patch System

   The system should be patched up to date. All relevant service packs and security patches should be applied. Periodic checks should be carried out to see if there are any vulnerabilities in the system, which should be rectified with fresh patches.

vi) Post Vulnerabilities

   Post Vulnerability test, if vulnerabilities aren't found, the system is ready to be used

vii) Install Anti Virus and Anti -malware

   A suitable anti-virus and anti-malware package should installed on the system to prevent malicious software introducing weaknesses in to the system.

viii) Configure Firewall

The system should be connected to the company's firewall.

ix) After all the above stems, the system will be ready to be used.

23) Vulnerability assessment and penetration testing.

Periodic Vulnerability assessment of critical systems of the company is to be carried out, necessary changes/ modification to be done to remove the vulnerability from the system.

24) Training and awareness programme.

The designated officer and the committee shall conduct training and educational sessions for employees to make them aware on building Cyber Security and maintaining basic system hygiene, to enhance knowledge of Cyber/ IT security policy and making them aware of the up-to-date Cyber Security threats. These training sessions shall take place Half Yearly.

25) SYSTEMS MANAGED BY VENDORS

Whenever the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of the company are managed by vendors and the company may not be able to implement some of the aforementioned guidelines directly, the company shall, from time to time, instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

26) Social Media Access Policy

We understand that social media networks (such as Facebook, Twitter, LinkedIn, Instagram etc.) play an important part in today's society and that the majority of our employees may use social media in some personal capacity.

It is important for all employees of the Parwati Capital Market Pvt. Ltd. (PCMPL) to be aware that much of the information exchanged within social media networks online or otherwise falls within the public domain, and the line drawn between what is considered to be personal and public is not always clear. It is also important to remember that information posted on social network sites can be easily traced and can generally be accessed at any time.

The purpose of this policy is to outline minimum standards regarding social media use and participation for all employees during their employment with the Parwati Capital Market Pvt. Ltd. (PCMPL)

- Employees should not post anything on social media networks that refers to their employment, the Company or any persons associated with the Company (e.g. other employees, directors, dealers, clients, suppliers, etc.) without the Company's express permission;
- Employees of the Company should not participate in social media networks in such a way that negatively impacts upon their effectiveness and productivity at work;
- When participating in social media networks, employees of the Company should ensure that personal comments do not bring the Company or any of its directors or its employees into disrepute;

- Any breach of this policy may result in disciplinary action, up to and including termination of employment.

27) Remote Access Policy

Purpose

The purpose of this policy is to define the rules and requirements for connecting to our organization's network from any host (computers, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

Policy

It is the responsibility of Parwati Capital market Pvt. Ltd. employees, dealers, vendors and agents with remote access privileges to corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection. General access to the Internet for recreational use through company network is strictly limited to our employees, dealers, vendors and agents (hereafter referred to as "Authorized Users"). When accessing our network from a personal computer, Authorized Users are responsible for preventing access to any company computer resources or data by non-Authorized Users. Performance of illegal activities through our company network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. Authorized Users will not use our networks to access the Internet for outside business interests. All remote access given to vendors and service providers are under supervision of the authorized person giving access, they will require to be on the screen and need to monitor the activities of the person taking remote access.

Connection Procedures

1. Secure remote access will be strictly controlled with encryption through Virtual Private Networks (VPNs)) and strong pass-phrases.
2. Authorized Users shall protect their login and password, even from family members.
3. While using our corporate owned computer to remotely connect to our corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control
4. Use of Remote resources to conduct company business must be approved in advance by the appropriate authority weather be Director/Compliance Officer/CISO.

PARWATI CAPITAL MARKET PVT. LTD.
KOLKATA

Compliance

Parwati Capital Market Pvt. Ltd. IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring (if applicable), business tool reports, internal and external audits, and/or inspection. The results of this monitoring will be provided to the Director/Compliance Officer/CISO.
All the softwares and hardwares are applied with only the necessary patches.
It is made sure that remote access is only provided under supervision.
Yearly cyber security awareness training is provided to make employees aware of the various cyber threats.
All data is backed up to help work seamlessly.
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Applicability

This policy applies to all company employees, dealers, vendors and agents with a company owned or personally-owned computer or workstation used to connect to our network. This policy applies to remote access connections used to do work on behalf of company, including reading or sending email and viewing internet web resources. This policy covers any and all technical implementations of remote access used to connect to our company's networks.

28) Cloud Computing Model

Parwati Capital Market Pvt Ltd recognizes the importance of cloud computing technologies for enhancing business agility, scalability, and cost-efficiency.

Definition:

IaaS refers to the provision of virtualized computing resources over the internet, including servers, storage, and networking components.

Governance, Risk and Compliance

Azure Governance helps to Build and Scale our apps quickly while maintaining control. We have fully governed cloud environments throughout our organization with Azure Blueprints

Selection of CSPs

Our Data is hosted in Microsoft Azure Datacenter in compliance with applicable legal and regulatory requirements issued by SEBI. Microsoft Corporation India is empanelled CSP under MeitY.Also have undergone SOC 2 and SOC 3 Reporting Structure as mentioned holding a valid STQC audit status.

PARWATI CAPITAL MARKET PVT. LTD.
KOLKATA

Data Ownership and Data Localization

As we are subscribed to a Iaas Structure we are the sole owners of our data and the Data resides within India at Central India Datacenter of Microsoft.

Responsibility of the Regulated Entity

In this arrangement, Microsoft are responsible for the security of the cloud, while we handle the security inside. Its a shared responsibility model of cloud security framework that outlines cloud providers' and customers' security obligations and responsibilities for ensuring accountability

Due Dilligence by the regulated Entity

Complied with national, regional, and industry-specific requirements governing the collection and use of data with help from Microsoft's comprehensive set of compliance offerings.
Verify technical compliance and control requirements with help from Microsoft's reports and resources for information security, privacy, and compliance professionals. To comply with laws and regulations, cloud service providers and their customers enter a shared responsibility to ensure that each does their part.

Security Controls

We have NSG Configured and Restricted Access to only our users. Use of multilayered, built-in security controls and unique threat intelligence from Azure helps us identify and protect against rapidly evolving threats.

Contractual & Regulatory Obligations

Microsoft Azure Legal Information

BCP, Disaster Recovery & Cyber Resilience

Microsoft's Enterprise Resilience and Crisis Management (ERCM) team oversees business continuity management and disaster recovery activities across Microsoft services and cloud offerings. 3 copies of Data are stored withing the Datacenter of Microsoft for Redundancy. Separate Offsite Backup is taken regularly.

Vendor Lock-in and Concentration Risk Management

Due to a lack of clarity on these issues, financial institutions may conclude that a risk averse posture dictates a multi-cloud strategy must be adopted. No regulatory guidance mandates a multi-cloud strategy. Rather, as with all forms of outsourcing, concentration risk is one of many risks that must be assessed, and customers must develop governance and have assurance plans in place to mitigate and manage such risks when using cloud services.

PARWATI CAPITAL MARKET [illegible]
KOLKATA

Standard Operating Procedure (SOP) for handling Cyber Security incidents

The Company is to follow the below-mentioned SOP for handling of Cyber Security Incidents which has been approved by the Board of Directors in its Meeting on O2-lun-2o22

STEP 1 - Upon identification of a Cyber Security Incident, the identifier (User, Staff, Employee, Dealer or any other individual should immediately inform the Chief Information Security Officer {CISO). In case the CISO is not contactable on immediate basis, the Designated Officer (DO) and the members of Internal Technology Committee (MITC) will be informed.

STEP 2 - Upon receiving the incident details from the identifier, the CISO, DO of MITC shall immediately verify whether the incident is falling under High / Medium /Low category as per the Cyber Security Incident Handling Process Document.

STEP 3 - All the incidents falling under the under-mentioned category shall be classified as a High Risk Incident irrespective of the fact whether they are intentional or unintentional

- Incidents that have financial implication
- Incidents that will/might have any impact on confidential organization data
- Incidents that have resulted into any kind of compromise of critical data like user ids, passwords, admin rights, unauthorized access etc.
- Any kind of virus, malware, ransom ware attacks effecting the information system

It is to be ensured that any kind of cyber security incident as mentioned in our Cyber Security and Resilience Policy shall be by default classified as a High Risk Incident. The degradation of these incidents into Medium / Low Risk Category shall he backed by sufficient recorded evidences along with the approval of CISO/DO/MITC.

STEP 4 - The below-mentioned actions shall be initiated upon identification of any Cyber Security incident:

- Immediate Reporting of Incident to CERT-IN by the CISO and in his absence by the DO or MITC. In case the incident is not reported to CERT-IN, proper documented reason for the same must be kept in record.
- Immediate Reporting of Incident to the Exchange(s), SEBI and any other Regulator(s) along with the reason of not reporting the Incident to CERT-IN
- Communicate with CERT-In/ Ministry of Home Affairs (MHA)/ Cyber Security Cell of Police for further assistance on the reported Cyber Security incident.

PARWATI CAPITAL MARKET PVT. LTD. KOLKATA

- If Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell, details need to be provided to Exchange and SEBI. If no, then the reason for not registering complaint shall also be provided to Exchange and SEBI.
- The details of the reported Cyber Security incident and submission to various agencies by the Members shall also be submitted to Division Chiefs (in-charge of divisions at the time of submission) of DO-MIRSD and CISO of SEBI.

The Designated Officer shall continue to report any unusual activities and events within 24 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter or in any other manner as specified by the Regulator from time to time.

CAPITAL MARKET PVT