Parwati Capital Market Pvt. Ltd. is a SEBI registered Stock Broker & Depository Participant and follows a system for IT Security with a view to ensure that the rules & regulations of regulators, government agencies, exchanges, depository and other authorities are complied with internal control and risk of the organization is managed in a smoother manner.

For this purpose the company from time to time has laid down certain Policies & guidelines. The Company has a compliance team led by Compliance Officer and a suitable back-office team to ensure smooth operations.

Parwati Capital Market Pvt. Ltd. recognizes that information security is a business responsibility shared by all members of the management team and that a management framework is required to initiate and control the implementation of information security within the organization.

Parwati Capital Market Pvt. Ltd. reserves to make changes in the Policy and Procedures as may be required from time to time and this Policy and Procedures will be reviewed every year.

The policy has been reviewed taken on records and approved by the board of directors of the Company at their duly conveyed meeting held on **06.06.2024.**

IT Infrastructure Management

The purpose of this IT Infrastructure Management policy is to define the guidelines and procedures for managing the information technology infrastructure of Parwati Capital Market Pvt Ltd. It aims to ensure the availability, reliability, security, and performance of the company's IT systems and infrastructure.

Roles and Responsibilities

IT Department:

a. The IT department is responsible for managing and maintaining the company's IT infrastructure.

b. They are responsible for ensuring the availability, reliability, and performance of the IT systems.

c. They must conduct regular risk assessments, vulnerability scans, and implement appropriate security measures to safeguard the infrastructure.

d. The IT department must monitor the infrastructure, identify and respond to incidents promptly, and conduct regular backups and disaster recovery tests.

Employees:

a. Employees must adhere to the company's IT policies and procedures.
b. They should report any IT infrastructure issues or security concerns to the IT department.
c. Employees should not attempt to modify or interfere with the IT infrastructure without proper authorization

Management:
a. Management must support and enforce compliance with this policy.
b. They should allocate appropriate resources for maintaining and upgrading the IT infrastructure.
c. Management should provide necessary training and awareness programs for employees to understand their roles and responsibilities.

Various policies / guidelines are as under : -

Audit Trail

Purpose

The purpose of this Audit Trail Policy is to establish guidelines and procedures for Parwati Capital Market Pvt Ltd. (referred to as "the Company") to maintain an accurate and reliable audit trail of all activities and transactions within the organization. This policy aims to ensure compliance with regulatory requirements, enhance accountability, and support effective risk management and internal control processes.

The audit trails maintain a record of all actions on resources by individuals and computing programs and processes. The purpose of the audit trails is round the clock tracking of resources usage, detailed monitoring of employee activity, real time event logging and so on.

Audit trails main objective is to keep track of activities which are performed in the system on regular basis. This helps in shooting the loop-hole areas of which logs are maintained.

Scope

This policy applies to all employees, dealesrs, and any other individuals who have access to the Company's systems, applications, or data. It covers all activities, processes, and transactions conducted within the Company, including but not limited to trading, investment advisory services, client onboarding, compliance monitoring, and any other relevant operational functions.

Storage of Logs

Logs are store in the system itself. Administrator can fix the time for backup of this logs. These logs will not overload the system as regular backup are maintained. Log retention period can be fixed by the Company based on the regulatory requirements as specified from time to time.
Logs should be stored on various backup media like hard disk, etc.

Review of Audit

Audit trails can be reviewed on weekly basis. But Company should not restrict review to certain time limit, it can review the audit trails as and when requirement occurs or it can be on regular basis also. Corrective action shall be taken based on audit trail information.

Data Retention

The Company shall retain audit trail records for a minimum period as required by applicable laws, regulations, and internal policies. The retention period may vary depending on the nature of the activity or transaction.

The designated personnel responsible for data retention shall ensure that the records are stored in a secure and easily retrievable manner to facilitate timely audits, investigations, and regulatory inquiries.

Backup and Restoration

Back up is an important aspect of computer data security. The backup for computers owned and operated by PARWATI CAPITAL MARKET PVT. LTD. (PCMPLTD). are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the database server, the application server, the mail server, and the file server.

It is to protect data in the organization, be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Backup –The IT Department will be liable for saving of files onto external device or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive - The saving of old or unused files onto external device or other offline mass storage media for the purpose of releasing on-line storage room.

Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server. The restoration process will be checked in every quarter in mock participation & will be the responsibility of senior official of the organization.

Daily Integrated back up of all data in database server, file server, and utility files including all patches, fixes and updates shall be taken on a regular basis.
Other servers like the application server, and operating system shall be carried out at least once a week.
Media: The media on which the backup shall be taken may comprise of External Hard Disks, Tapes, or any other media being used by the company.
Back up data shall be stored on site in a fire proof cabinet and a copy of the same shall be at maintained at an offsite location.

The IT department In-charge shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

Following daily procedures have been put in place to co-ordinate day to day activities:

Beginning of day process where it is checked that the servers are properly started, connectivity check is done, login is properly done, files are uploaded, engines are started and after error free start reported to administrator via mail.

End of day procedures where at the end of day proper trade and order backups are taken along with all the necessary logs and reported to administrator via mail.

Weekly Back up process is done to secure Logs generated and back up of application server.

Verification and Testing

The integrity of the data shall be verified at the time of daily back-up by enabling the integrity check function. The data stored on the back-up server may be tested at the time of mock trading.

Archives
The data, if necessary, shall be archived at the end of 90 days.

Password Policy

A password policy is a set of guidelines and requirements that organizations or systems implement to ensure the security of user passwords. These policies aim to prevent unauthorized access, protect sensitive information, and minimize the risk of security breaches.

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.

General

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every one month. The recommended change interval is every fourteen calendar days.
Passwords shall not be placed in emails unless they have been encrypted / the network traffic is encrypted.

Trading Application Password

The Password is masked at the time of entry.
System mandated changing of password when the user logons for the first time.
Automatic disablement of password on entering erroneous password on three consecutive occasions.
Password shall be alphanumeric and neither only alpha nor only numeric.
Password shall be changed at an interval of fourteen calendar days.
Password shall not be same as last eight passwords.
Password shall not be same as User Login ID.

Password shall be encrypted in the database so that it cannot be viewed by any one at any point of time.
The session shall be reinitialized upon modification of password by the user.

Application Software Policy

The purpose of this Application Software Policy is to establish guidelines and procedures for the management, usage, and security of application software at Parwati Capital Market Pvt Ltd. This policy aims to ensure the efficient and effective utilization of application software while maintaining the integrity and security of company resources.

Software Installation and Updates

1. All software installations and updates must be performed by authorized personnel following the approved procedures.

2. Only software obtained from trusted and reputable sources should be installed on company devices.

Software Policy:

We use Algo driven software's of empanelled vendors of exchanges which have their prior approvals with exchange having proper documentation and version numbers.

Any changes is updated and checked before moving to live environment at vendor end.

Application patches policy:

We use applications of empanelled vendors, they provide us with patch upgrade as per the requirement.

Application related patches are thoroughly tested by the IT team at vendor end.

Observations, if any, are logged and upon fixation of the same, the same are tested again and then the patches are released to the live environment.

Network Security

Network Administration

Monitor Network Performance, Server's power supply and UPS, cooling temperature and smoke detector by time to time

Auto update the virus definition scan/detection/removal at all levels of entry point appropriate.
Monitor Backup activities.
Maintain Network cabling.
Review and approve all planned network changes and updates.
Schedule downtime and notify all users sufficiently in advance.

System Administration

Installation and configuration of Server Operating Systems.
Adding & configuration of new workstations.
Creating, Issuing, Deactivating User-Ids and associated groups and passwords.
Implementing procedure to remove virus and unauthorized access.
Ensuring documentation of all hardware and software resources.
Install and update software & hardware & Network Operating System patches.

Database Administration

Tuning the database.
Taking periodic backup of database.
Ensuring proper procedures for labeling back-ups.
Ensuring system backup is available off-site.
Testing the backups periodically and applying recovery procedures whenever required.

Security Incident and Event Management

Parwati Capital Market Pvt Ltd is committed to maintaining the security and integrity of its information systems and assets. This Security Incident and Event Management (SIEM) policy outlines the guidelines and procedures to effectively manage security incidents and events, ensuring timely detection, response, and mitigation of any potential threats or breaches.

The purpose of this policy is to establish a framework for incident and event management within Parwati Capital Market Pvt Ltd.

Incident and Event Management Roles and Responsibilities:

Chief Information Security Officer (CISO):

- Oversees the implementation and compliance of this policy.

- Ensures appropriate incident response and investigation procedures are in place.
- Facilitates training and awareness programs related to incident and event management.
- Coordinates with relevant stakeholders to address security incidents and events effectively.

Incident Response Team:

- Comprises members from IT, information security, legal, human resources, and other relevant departments.
- Responsible for responding to security incidents promptly, assessing their impact, and initiating appropriate actions.
- Conducts incident analysis, investigation, and documentation for further improvements.

IT Department:

- Monitors security events and incidents using the SIEM system.
- Implements security controls and measures to detect, prevent, and respond to security incidents.
- Collaborates with the Incident Response Team to investigate and resolve incidents.

Information Security Policy

The machines are protected with antivirus.
Password Protection: We assign the dealer a user name and a password for logging into the trading system. The combination of login ID & Password authenticates their identity from our secured database.
The algo trading system also has a feature whereby the transaction password expires every 14 days. Thereby, we force the dealer to change his/her password every 14 days for ensuring high security for all the transactions.
We continuously educate our users about their Identity Protection.
We have a robust risk management system in place. We have a dedicated surveillance and monitoring team, where experienced personnel are continuously monitoring terminal operations throughout the trading hours. Each dealer is under continuous watch as regards exposures, margins, turnover, market to market profits/losses and so on.
We have hosted our servers at colocation services of NSE which has all security features of access.

Software Change Management Policy

The purpose of this policy is to ensure that all changes to software systems within Parwati Capital Market Pvt. Ltd. are managed in a controlled and efficient manner, minimizing risks, and maintaining the integrity, security, and performance of our systems.

This policy applies to all software systems, including trading platforms, databases, financial applications, and system software used by Parwati Capital Market Pvt. Ltd. It encompasses all types of changes, including bug fixes, feature enhancements, upgrades, and new software deployments.

User Management and Access Control

The User Management Policy outlines the principles and guidelines for managing user accounts and access privileges within Parwati Capital Market Pvt. Ltd. This policy aims to ensure the security, integrity, and confidentiality of company resources and information.

Access control standards for information systems shall be established by management and shall incorporate the need to balance restrictions to prevent unauthorized access against the need to provide unhindered access to meet business needs.

The purpose of the Access Control Policy is to define a set of computer connection classes, designed to minimize the exposure to PARWATI CAPITAL MARKET PVT. LTD. (PCMPLTD). from destruction, theft and loss of data.

Access to the resources on the network shall be strictly controlled to prevent unauthorized access.
Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.
Access to systems and their data shall be restricted to ensure that information is denied to unauthorized users.
Access is to be logged and monitored to identify potential misuse of systems or information.
Remote access control procedures shall provide adequate safeguards through robust identification, authentication and encryption techniques.
Passwords shall not be placed in emails unless they have been encrypted / the network traffic is encrypted.
Default passwords on all systems shall be changed after installation.

User Creation / Deletion

User Account Creation

1. User accounts will be created for employees, dealers who require access to company systems and resources.
2. Account creation will be based on the principle of least privilege, ensuring that users are granted only the access necessary to perform their job functions.
3. Requests for user accounts must be submitted through the designated channels and approved by the appropriate authority.

The Administrator will ensure that new user ids were created / and also will ensure the deletion of user ids, not in used and will ensure that the id's are unique in nature. The request for new ID's creation or any modification changes to be made will be sent to administrator by support team via mail and the Administrator will process the same & confirm the same to support team via mail.

User Disablement

The Support Team will give the request for any disablement of user over mail to Administrator & the Administrator will ensure that non compliant users are disabled & will inform the support team.

User Management System

The System Administrator will ensure that the user id's are reissued as per the NSE guideline.

Access Control

1. Access privileges will be granted based on the principle of least privilege, granting users the minimum level of access required to perform their duties effectively.
2. User access will be reviewed periodically, and access privileges will be modified or revoked as necessary.
3. Access to sensitive systems and data will be restricted to authorized personnel only.
4. User access to systems and resources will be protected by strong passwords and two-factor authentication where applicable.
5. User credentials (e.g., passwords, access codes) must not be shared, and users are responsible for maintaining the confidentiality of their accounts.

Locked User Accounts: Users whose accounts are locked are unlocked only after proper unlocking requests are made by support team to the System Administrator.

Risk Management System

A Risk Management System is integral to an efficient Risk System. As a PRO trading firm we have put in place comprehensive risk management system, which is constantly upgraded as per the Exchange, SEBI & PMLA norm and also as per Market Movement.

Parwati Capital Market Pvt. Ltd. (PCMPLTD), is a Proprietary Trading entity, conducts its business operations based on sound Risk Management Policies to pursue prudent business practices and, for providing hassle free trading facility to its employees. The function of Risk Management being an ongoing exercise is reviewed periodically and necessary measures are initiated to enhance its overall effectiveness.

Human Resource Deployment -

New people are deputed as Dealers with specific roles. They work in tandem with the entire team, and are specially deployed to undertake planned actions in case the anticipated risks come true.

Algorithmic Trading Policy

The purpose of this policy is to establish guidelines and procedures for the development, deployment, and management of algorithmic trading systems at Parwati Capital Market Pvt. Ltd., ensuring compliance with regulatory requirements and mitigating associated risks.

All or Algorithmic Trading software's are developed by empanelled vendors and we don't use any In-house software's. The software's are managed and rigorously tested by the vendor's. Patch updates/ Software version updates with respect to the Exchange compliances are provided by the vendor.

Trading Limits

As a PRO Trading Firm PARWATI CAPITAL MARKET PVT. LTD. (PCMPLTD) Limits to the Dealers are approved by the Management only. No administrative rights are given to Dealers. Checks such as Single Order Quantity and Single Order Value Limits,

User Order / Quantity limit, User / Branch Order value Limit, Order Price limit, Spread order quantity and value limit, M to M are in place.

Risk Control:

All CTCL's and algo software's have Limit Price Protection(LPP), Market Price Protection(MPP), Circuit Breaker Check, Market Depth Check.

IT Infrastructure Planning and Device Ageing Policy

At Parwati Capital Market Pvt Ltd, we recognize the critical role of a robust IT infrastructure in supporting our business operations
This policy establishes guidelines for IT infrastructure planning and the management of device ageing within the organization. The objective is to maintain a reliable and secure IT environment while proactively managing the lifecycle of our technology assets.

Device Ageing:

a. The IT department shall maintain an inventory of all technology assets, including servers, computers, laptops, networking equipment, printers, and other relevant devices.

b. Each device shall be tracked and monitored throughout its lifecycle, from acquisition to retirement.

Devices that are beyond their recommended service life or pose a significant security risk due to outdated software or hardware vulnerabilities shall be promptly retired or replaced.

Data Migration and Disposal:

a. Prior to retiring or replacing devices, the IT department shall ensure that all sensitive and business-critical data is securely migrated to new devices or storage systems.

b. Data disposal procedures shall be followed to permanently remove data from retired devices, adhering to data protection and privacy regulations.

c. The IT department should implement appropriate data backup and recovery mechanisms to safeguard against potential data loss during migration or disposal processes.

BCP DR Plan

As a PRO Trading firm PARWATI CAPITAL MARKET PVT.LTD. (PCMPLTD) has implemented a Business Continuity Plan from its Branch office to ensure the continuation and/or rapid recovery from failure or interruption of business if any Disaster occurs in its main office, A dedicated link from Branch office to NSE Co-Location is there so that connection can be established and all the servers can be connected & the business can continue smoothly. Periodic drills are carried for periodic contingency testing.

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 (cell phones, 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. For additional information regarding our remote access connection options, including how to obtain a remote access login/VPN, anti-virus software, troubleshooting, etc., see our IT technical lead.

Connection Procedures

1. Secure remote access will be strictly controlled with encryption through Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see our company's Encryption Policy and the Password Policy.
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 by Director/Compliance Officer/CISO.

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. An employee found to have violated this policy may be subject to disciplinary action, up t o 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 intranet web resources. This policy covers any and all technical implementations of remote access used to connect to our company's networks.

Capacity Management Policy

Capacity management is a process used by organizations to ensure that their IT resources and services are right-sized to meet current and future demands in a cost-effective manner. It involves planning, monitoring, and optimizing the performance and capacity of IT infrastructure to ensure that resources are utilized efficiently and can support business activities effectively.

Purpose

The purpose of this policy is to establish a framework for managing the capacity of IT resources to ensure they are sufficient to meet business needs, optimize resource utilization, and maintain performance levels.

Scope

This policy applies to all IT infrastructure, applications, services, and resources managed by the Parwati Capital Market Pvt. Ltd. It covers the processes involved in capacity planning, monitoring, and optimization. Parwati Capital Market Pvt. Ltd. will implement and maintain a capacity management process that ensures IT resources are effectively managed and optimized to meet business requirements, support service levels, and control costs

Roles and Responsibilities

- **IT Leadership**: Approve and oversee the implementation of the capacity management policy.
- **Capacity Manager**: Develop, implement, and maintain the capacity management processes. Ensure alignment with business objectives and performance requirements.
- **IT Operations**: Monitor IT resource utilization and performance. Provide data for capacity planning and management.
- **Business Units**: Provide input on business plans and growth projections to inform capacity planning.

Conclusion

This IT Policy of Parwati capital Market Pvt. Ltd. ensures that the organization's IT resources are aligned with business needs, optimized for efficiency, and prepared to support future growth. By following this policy, the organization can maintain high performance, control costs, and effectively support its strategic objectives.

Privileged Identity Management

Privileged Identity Management (PIM) is a security practice that involves managing and controlling privileged accounts and access rights within an organization. Privileged accounts typically have elevated permissions and privileges that allow users to perform critical or sensitive tasks, such as system administration, network management, or accessing sensitive data.
Privileged Access is approved to the following people:

Sarad Daga: Access to organizations IT systems, Back office software's, & data, Banking Details.

Chandra Prakash Srivastava: Access to the IT Servers, and cloud for Accounting Purpose.

Karna Kant Damani: Access to organizations IT systems such as the servers, routers etc. to check for to cyber security breach.

Soumyadipto Ghosh: Access to organizations IT systems such as the servers, routers etc. to provide seamless working environment at the organization.

Satrughan Sharma: Access to organizations IT systems such as the servers, routers etc. to provide seamless working environment at the organization.

Prasenjit Das: Access to organizations back-office software's and data.

Shyam Sundar Basu: Access to organizations back-office software's and data.

Access to Privileged Information is provided to the other people on a case-to-case basis with supervision from the Privileged Access approved users.

Guidelines for prevention of Business Disruption due to technical glitches & Standard Operating Procedures (SOP) to be adopted upon incident of Technical Glitches.

I. Objective

The objective of this guideline is to outline the technology infrastructure and system requirements that Parwati Capital Market Pvt. Ltd. should put in place to prevent any incident of business disruption resulting from technical glitches. These guidelines also prescribe the Standard Operating Procedures (SOP) for reporting of technical glitches to exchanges, handling business disruption, management of such business disruption, including declaration of disaster and framing of provisions for disciplinary action in case of non-compliance in reporting/inadequate management of business disruption.

II. Definition

a) **"Technical Glitch"** shall mean any malfunction of the systems including malfunction in its hardware or software or any products/services provided by the Company, whether on account of any inadequacy or non-availability of infrastructure/ network/ other systems or otherwise, which may lead to business disruption.

b) **"Business Disruption"** shall mean either stoppage or variance in the normal functions /operations of systems of the Company, due to a technical glitch, w.r.t login, order placement (including modification & cancellation), order execution, order confirmation, order status, margin updates, risk management, for a continuous period of more than 15 minutes in any segment of the Exchange.

III. Preventive Measures

i System Controls & Network Integrity

- ESET endpoint antivirus is deployed and available at primary site for all critical systems including network and data center infrastructure.

ii. Backup and Recovery

- Load controller is deployed and when any of the link is down it automatically switches to another link so that it does not hamper the business.

- The Recovery Time Objective (RTO) i.e., the maximum time taken to restore the operations, and the Recovery Point Objective (RPO) i.e., the maximum tolerable period for which data might be lost should be minimal, for each of the business processes/services.