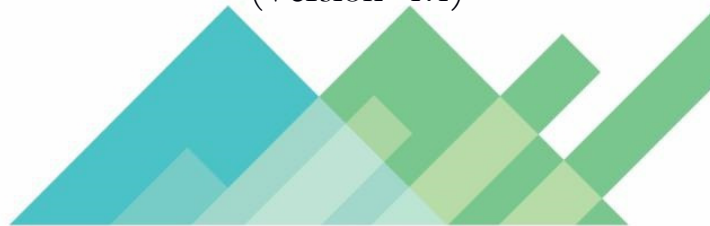


# **Cyber Security Policy**

(Version- 1.1)



## Document Control

<b>Document Name</b>	Cyber Security Policy
<b>Abstract</b>	This document describes the list of authorized software, IT Policy & Guidelines and System Architecture & Development Guidelines at <b>Mathisys Advisors LLP</b> .
<b>Security Classification</b>	Internal
<b>Location</b>	Gurgaon, Haryana, IN

Authorization			

Amendment Log				
Version	Modification Date	Section	Approver	Brief description of change

Distribution list	
Information Technology Co-Ordinator	
Information Technology Team	
ISMS Core Team	
Auditors (Internal & External)	

### Escalation Contact Details

Level	Name	Email	Telephone
1 <sup>st</sup> Level Contact	Sudhir Pant	Sudhir.pant@mathisys-india.com	+91-8218399669
2 <sup>nd</sup> Level Contact	Amit Kumar	Amit.kumar@mathisys-india.com	0124-2570702
3 <sup>rd</sup> Level	Gagan Tiwari	Gagan.tiwari@mathisys-india.com	0124-2570703



S no.	<b><u>Topic Covered under this Policy</u></b>
1.	Statutory mandate
2.	Objective of the framework
3.	Purpose and Scope-
4.	Designated officer
5.	Constitution of technology committee
6.	Protecting information technology-
7.	Information technology resources
8.	Staff and technology
9.	Third party access
10.	Maintaining records
11.	Password management
12.	Information reporting-
13.	Data backup and retrieval, audit trails-
14.	Cyber security incident response plan
15.	Cyber security & cyber resilience framework
16.	System architecture & development guidelines
17.	Enforcement
18.	Responsibilities of employees, members, and participants
19.	Periodic review and acceptance

## Statutory mandate-

This framework is formed by the requirements of the SEBI Circular *SEBI/HO/MIRSD/CIR/PB/2018/147 dated 03.12.2018*, and Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants-Clarifications SEBI Circular *SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated 15.10.2019* and modification in Cyber Security and Cyber Resilience Framework, Circular No. *SEBI/HO/IMD/DOF2/P/CIR/2022/81. Dated 09.06.2022*. and updated from time to time.

## Objective of the framework

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

In Addition to the above Cyber security policy shall detect, prevent and mitigate Cyber-attacks and threats which attempt to compromise the Confidentiality, Integrity and Availability(CIA) of the computer systems, networks, and databases (Confidentiality refers to limiting access to systems and information to authorized users, assuring integrity that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the system and information authorized users). The 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 operations during, and recover from, a cyber-attack.

## Applicability-

Provisions of the said circular and framing of cyber security and cyber resilience policy are required to be complied with Mathisys Advisors LLP registered with SEBI.

## Purpose and Scope-

This document sets out the way in which the business uses, develops and maintains Information Technology (IT) to assist in the achievement of the Objective and Goals of the business.

The purpose of this policy is to ensure: -

- The provision of reliable and uninterrupted IT services.
- The integrity and validity of data.
- An ability to recover effectively and efficiently from disruption.
- The protection of all the IT assets of the organization including data, network, software and hardware.

This policy also covers the various steps and processes we expect to have in place to ensure we have an effective Information Security system to prevent unauthorized access, use and exploitation of data we hold on our clients and on our business practices and process.

All staff and Authorized Representatives must be familiar with and comply with this Policy and Procedure, understand the importance the business places on the effective operation of our Policies and Procedures and are encouraged to look for improvements to our procedures.

## UPDATES-

These Policy and Procedures are updated on a regular basis. Any material changes to these Policy and Procedures will be advised by management either via email or at our regular Staff meetings. This document and associated forms etc. are accessible in soft copy via our computer network. We do not store these documents in hard copy. All information can be immediately accessible on the computer network and will be guaranteed to be up to date at all times.

When you see the opportunity to improve a procedure, kindly make the suggestion known to your Manager/Supervisor as we all have a responsibility to improve our standards, individuality and as an organization.

## DESIGNATED OFFICER

The company nominates **Mr. Amit Kumar** as the Designated Officer of the company 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.

## CONSTITUTION OF TECHNOLOGY COMMITTEE-

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

Sr. No.	Name of the Committee Members	Designation of the Members
1	<b>Nihit Gupta</b>	<b>Chairman</b>
2	<b>Gagan Tiwari</b>	<b>Member</b>
3	<b>Amit Kumar</b>	<b>Designated Officer</b>

Such committee shall on a half-yearly basis review the implementation of the Cyber Security and Cyber Resilience policy. Such review shall include but is not limited up to, reviewing current IT and Cyber Security and Cyber Resilience capabilities, setting up goals for a target level of Cyber Resilience, and establishing plans to improve and strengthen Cyber Security and Cyber Resilience. The review shall be placed before the Board of directors for taking appropriate action(s) if required. The Designated officer and the technology committee shall periodically review instances of cyber- attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

The technology committee in accordance with the provisions of the said circular and formed hereinafter this framework, shall ensure that this framework considers the principles prescribed by the National Critical Information Infrastructure Protection Centre (NCIIPC) of the National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.

## **PROTECTING INFORMATION TECHNOLOGY-**

Where possible and practical key computer hardware is to be located in secure areas with access limited to relevant staff. Where cost effective such equipment is to be protected from power surge by hardware. Access to the secure location is to be limited to few staff whose access is per-approved by the manager or the person authorized to do so.

The Information Technology Co-Ordinator (ITC) will allocate responsibility for securing the software and hardware assets wherever it is stored. A backup person should be organized to cover times when the primary person is unavailable because of holidays, illness etc.

Special care needs to be taken with the security processes for all portable electronic equipment or remote equipment with the ability to access our network or to store organization data. Specifically, all such equipment must have a commercial grade password to be able to access the machine. In the event of any such equipment lost or stolen, staff and representatives are to immediately advise ITC who will take necessary steps to deactivate the specified equipment's access to our network. This will include changing any network Wi-Fi passwords as well as user passwords for any staff that may have used the lost/stolen equipment.

In addition, all hardware that has the ability to access our network remotely must be able to be locked out of the network regardless of the password access provided to the network. In other words, there must be hardware security in place as well as the software security.

The business operates Anti-Virus software across our network and as part of the induction process new staff and representatives are trained in the identification of potential virus and preventing the systems whenever virus has been detected.

### **a. Anti-Virus Management**

- Official version with latest virus definition files of anti-virus software shall be installed on all workstations, laptops and servers. The anti-virus software shall be updated by obtaining the latest updates from the antivirus vendor and distributed promptly across the organization.
- Personal computers (e.g., laptops, desktops) shall be scanned on regular basis for viruses.
- System administrator shall run anti-virus software on all folders on server on a regular basis.
- All information or files downloaded from the Internet onto a workstation and all mail attachments shall be scanned for viruses before opening them.
- Any electronic information being brought into organization's IT environment e.g., diskettes, tapes etc. shall be scanned, prior to use. vi. If a virus attack is suspected, suspect personal computer shall be immediately removed from the network and the process as per the Incident Management Policy shall be followed.

### **b. For control on Virus Prevention and Protection**

Anti-virus software should be selected and configured in such a way that it should be capable of:

- Should be able to identify and vaccinate accurately all known viruses, macros and their variants
- Capability to scan and identify new viruses and macros depending on their signature patterns and viral activities
- Scan proactively and reactively iv. Capability to vaccinate or recover original file rather than deletion
- Alert and messaging facility to notify users and administrators about the virus infection
- Anti-virus software should support the operating systems used in the organization
- The anti-virus software should be capable of scanning; memory, removable media, local and network drives, BIOS, all types of the file extensions, emails, internet pages, downloads etc.
- Anti-virus should have minimum implementation issues at both the server and user end

### **c. Anti-virus software for End Users**

Anti-virus software at desktop should be configured in such a way that it should:

- Invoke automatically at the start-up, scan for memory and all data storage devices connected to the machines
- Scan all incoming emails and attachments as and when they arrive
- Scan all incoming downloads and web pages visited by the users
- Scan all types of supported file extensions including compressed and executable files

Anti-virus software at user end should support scanning of adware/spyware

- It should be possible to update the anti-virus software manually and automatically. Periodic update can be enforced during initial login using start-up scripts.
- If any machine is infected, it should automatically notify the details of such infection to the antivirus administrator. The antivirus administrator should present the weekly status report highlighting virus outbreaks to IT Co-Ordinator.
- The antivirus software should be configured such that users cannot change the configuration settings

All users are responsible for maintaining a virus and spyware free environment. The following standards are in place to assist users in meeting this responsibility:

- Up-to-date virus/spyware-checking programs approved by IT Coordinator should be continuously enabled on all servers and other devices connecting to network systems.
- Since viruses and spywares are often complex and sophisticated, users should not attempt to remove them without expert assistance. Users shall contact the IT within the organization for assistance.
- All software and files downloaded from non-organization sources via the internet or other sources should be scanned with anti-virus and spyware
- Users should scan all diskettes and other media like pen drives for viruses and spyware prior to using the media



#### **d. Other major steps to be taken-**

- Firewalls have been installed within the computer network to protect the IT system from attack from external sources.
- Under no circumstances staff or representatives are to introduce software programs or external data to the IT system without prior approval of the ITC.
- To ensure the security and integrity of all our data that the business will rely on going forward must be stored on selected resources to enable the effective back up and subsequent recovery of such data in the event of a disaster.
- Any disaster that impacts our Information technology systems has the potential to have a catastrophic result for the operation of the business.
- To ensure the business continues to have the IT capability to meet the needs of the business, an inventory of all IT hardware and software is maintained by the business as part of our Asset register.
- Where we have a Wi-Fi network it is to be secure, encrypted, and hidden. To hide our Wi-Fi network the wireless access point or router is to be set up so that it does not broadcast the network name, known as the Service Set Identifier (SSID). There will also be a commercial grade password applied to the Wi-Fi router.

## **INFORMATION TECHNOLOGY RESOURCES**

We have nominated an Information Technology Co-Ordinator (ITC) as well as system engineers where relevant with the responsibility for the management and maintenance of all IT systems within the business.

The ITC's will be provided with the necessary training to be able to effectively perform their role.

We have will also engaged a reliable IT provider to provide professional service, support and expertise to the business to ensure our IT systems operate to an industry standard and to assist the ITC in technical areas that are beyond experience and expertise of our ITC.

### **ROUTINE ACTIVITIES**

The day-to-day management of our IT infrastructure and effective implementation of this policy rests with our ITC. The specific skills, roles and responsibilities of the ITC include: -

- Controlling all staff and representative access to the Information Technology environment including passwords.
- Ensure staff and representatives are only provided access to IT areas / data required to perform their role and that a workable hierarchy of authority is in place so that staff and representatives are only authorized to perform tasks which they are required / trained and expected to perform.
- Ensuring staff and representatives store all relevant data on the nominated data storage devices.
- Server backups are completed as per schedule and before any major software or hardware changes are implemented.

- Any firewall that has been installed operates on all network to ensure that the systems and network is protected.
- Selecting/Installing/Replacing/Maintaining IT hardware.
- Ensure access to data and communication servers and control tables is limited to the ITC and delegated staff.
- Ensuring default passwords on software or hardware supplied from vendors is updated immediately upon receipt.
- Ensuring periodic update of password of any software and hardware which are protected by password.
- Ensure that no software/hardware is able to be set to have “auto password complete” activated in any situations.
- Maintaining relevant IT records.
- Ensure access for departing staff and representatives is removed accordingly.
- Develop and maintain standard specifications for all hardware and software utilized within the business.
- Develop a thorough understanding on Disaster Recovery Procedures and implement work practices that are conducive to an effective recovery from a disaster.
- Consider the cost /benefit and implement where appropriate routine Penetration Tests on all external facing software. Penetration Testing is an authorized attempt for certified ethical ‘hackers’ to breach your system
- in order to identify its vulnerabilities and to safely close any flaws that real Cyber criminals may exploit.
- Maintain full details of computer network configuration, specification and software for use in the event of a disaster.
- Review the currency and appropriateness of our hardware and software, response times, downtime and any complaints received from staff regarding our Information Technology resources.
- Nominate and train a replacement person responsible for Back Up procedures when the ITC will not be available.
- Check that all organization equipment which is physically on the same network as our Servers has had all capability of loading CD’s/DVD’s/USB Drives removed or deactivated.
- Maintain a record of all hardware and software that has the ability to access our network remotely and regularly review the usage of such hardware to assess whether such ongoing access is warranted and relevant.

## **DISASTER RESPONSE ACTIVITIES**

- To see that full IT functionality is restored in the minimum time, with particular focus on an effective restoration of data from our back up facilities.

- Liaise with critical suppliers to determine the causes of failure and to develop plans to restore functionality.
- Liaise with the ITC and the Responsible Manager(s) to update them on status and to plan the return to normal business, as systems become available.

## **STAFF AND TECHNOLOGY**

The majority of staff and representatives have access to a PC or related equipment. The organization has computer facilities and systems with internet access for e-mail and research. Access to these facilities is for predominantly business purposes only and not for private matters. Our view is that all data, information, messages etc. that are transacted over our network and hardware is not subject to any privacy restrictions that might usually apply to individuals.

Any usage of Our IT equipment to access, create, store or otherwise facilitate the use of pornographic, sexually explicit material or other data that would be considered inappropriate by community standards is a Serious Breach of our Policy and Procedures and will result in immediate termination for the staff or representative involved.

The ITC will randomly monitor traffic to and from the server as well as the overall network. The ITC will also advise all staff and representatives of any common viruses that are known to be impacting the resources.

PCs and notebook computers must not be left unattended for long periods while signed-on. Only authorized software's to be installed on PC and Notebook. Confidential data must be stored securely when unused. All PC and Notebook computers are protected with antivirus.

Users are only permitted to access electronic information and data that they require to perform their duties. If the users find that they have access to information that they are not concerned with, IT Co-Ordinator should be intimated of the same immediately.

If confidential information is lost, either through loss of a notebook computer, backup media or other security breach, IT must be notified immediately. All computers must be switched off at the end of the day.

### **Personal use of computer systems**

While notebook computers and PCs are provided to organization personnel for business use, it is not acceptable to use them for personal use. Action will be taken if personal use of notebooks and PCs a) interfere with the user's job commitments or b) have a detrimental effect on the computer or network's performance.

Personnel must not use organization's systems or the Internet connection provided for commercial activities that are not related to the business of the organization.

### **PC and Notebook Security**

PCs and notebook computers must not be left unattended for long periods while signed-on e.g. during lunch, coffee breaks etc. Users must either logoff, lock workstations or activate a password-controlled screensaver if they are leaving their PC for extended periods of time. If a screen saver is used then it should be set to activate by default after 15 minutes of inactivity.

### **Internet and E-mail**

- All access to the Internet from organization network will be via an approved channel that will be secured by a firewall.
- The organization reserves the right to review, audit, intercept, access, block access to sites deemed unacceptable and disclose all access to the Internet. This includes emails sent and received in addition to websites visited and files downloaded from the Internet.
- Users must not publish data on the Internet without the express prior written permission of ITC. This prohibition includes the posting of information to chat-rooms, bulletin boards or news groups.
- The use of, or access to, web-based e-mail systems, such as 'Hotmail,' for business purposes is forbidden.
- Email users must exercise caution with any external attachments other than those received from a trusted source, as these attachments may contain a computer virus.
- Users must not represent themselves as another individual in electronic communications.
- Email users must be aware of the risks associated using email to send confidential or commercially sensitive information.
- Users must ensure that documents attached to emails are not copyright protected.
- Email messages must be appropriate and professional.
- As email is a form of publishing and covered by relevant publishing Acts, libelous and defamatory material is not permitted.
- Users must not use email for transmitting data of a personal nature related to a third party.
- If any person receives email, which they deem to be inappropriate, offensive or illegal, they must inform ITC. Immediate reporting of incidents facilitates more successful identification of the source and other details.
- All emails that are sent externally must carry a standard disclaimer of the organization. Users must not attach their own disclaimers to emails.

### **Unsolicited Communications**

Email - Messages that contain text which indicate that they may have come from an unsolicited source should be reported to IT for further action.

### **Telecommunications**

Remote Access can be defined as "Access to IT resources or data from a location external to organization". This access may be by a third party or an employee who is located off-site. For cost and security reasons remote connections must be closed as soon as the purpose of remote access has been met with.

Telephone numbers that are used to access organization's computers must not be listed in public telephone directories and must not be disclosed to unauthorized personnel.

## **Third Party Access-**

Third Party Access can be defined as "The granting of access to the organization IT resources or data to an individual who is not an employee of the organization". E.g., Software Vendor who is providing technical support, Contractor or consultant, Service Provider etc. Further requirements for granting Third Party Access are: -

- Risk analysis
- Approval by Data Owner
- Approval by the ITC.

## **Software Licenses**

Copyright stipulations governing vendor-supplied software must be observed at all times. IT maintains records of software licenses. Software that is acquired on a trial basis must be used in accordance with the vendor's copyright instructions. All software developed within the organization is the property of the organization and must not be copied or distributed without prior written authorization from the ITC. The unauthorized installation of software on Company personal computers is forbidden.

## **Data Backups**

Users must always save data and files on the network as opposed to the local hard disk. This ensures that regular backups are taken and are available for recovery purposes. Users should be aware that data saved on the local hard disk is not backed up by IT. IT takes regular backups of the main servers which they manage.

## **Copying of Software or Documents**

The copying of software or documents, which are copyrighted, is an offence. Pace Group has a policy whereby only licensed media is used within the organization. If you require additional software contact, ITC ensure that the relevant licensing agreements are complied with.

## **Damage to IT Equipment**

Intentional or threatened damage to data or IT infrastructure will not be tolerated. While in your possession you must take the necessary precautions to protect data and equipment provided to you.

## **Collection of Personal Information**

If users have access to personal information, users must ensure that it was obtained fairly, is accurate, protected against unauthorized disclosure, used only for the purpose(s) for which it was collected and is held no longer than is necessary for that purpose(s).

## **Fire Detection / Prevention**

The Server Rooms must be fitted with smoke/fire detectors and fire extinguishing equipment, which should be set to automatic operation when the computer room is left unattended for long periods. Fire detection and prevention equipment must be tested at least twice a year.

### **UPS / Backup Generator**

The entire Server room and the equipment's housed within it must have a UPS backup to protect against power surges/failures. The UPS and generator must be tested every 1 month.

### **Vendor Management**

All vendor-maintained equipment and software required to conduct the business of the organization must have formal support and performance contracts. ITC shall perform annual examinations of all information systems vendors who are actively maintaining the organization production environment. The examinations will assess potential risk, as sociable with both individual vendors and the industry as a whole.

All vendors receiving a non-satisfactory review shall undergo appropriate monitoring and shall take necessary corrective action.

## **MAINTAINING RECORDS-**

- The ITC is responsible to keep the inventory of hardware and software assets being used in the infrastructure. This inventory is crucial in planning the operations and assigning resources to the users whenever needed.
- The ITC should make sure the inventory being maintained is up-to-date by inspection and periodic updation. Staffs are trained to report about the installation, deployment of equipment, replacement of faulty equipment etc. to the ITC.
- Along with the hardware assets software assets like license keys of Operating systems, installed Antivirus and other software are also been maintained. This is helpful in renewal of license and vendor service contracts before the expiry of the product which ultimately result in the smooth running of the business.

## **CREATING MAINTAINING AND DELETING USERS**

- New staff and representatives need to be added as new users to the network, and just as importantly, old staff and representatives need to be removed as soon as they leave the business.
- The ITC is responsible to add new users and remove users to/from the network.
- The system for adding new users should enable a new user to be added to the network so they can be productive from the day they start work (without having to use someone else's password to access the network).



- The ITC maintains a central registry of passwords to business-critical files or applications, or to retrieve passwords from departing employees. For example, staff member may have password-protected individual data that the business will need.
- The person who oversees the departure of a staff member is responsible for informing the ITC that the employee is leaving. The ITC is responsible for disabling that user from the network as soon as they receive notice.

## **PASSWORD MANAGEMENT- CREATING AND RE-SETTING PASSWORDS**

- All new users on the network will need a password that they can change for their own needs. And whether we like it or not, users forget passwords and can be locked out of network. The ITC should be able to re-set the password of someone who is locked out within a very short time.
- The network operating system and all sub systems should be set up so as to require users to change their network password regularly. Password rules (eg. how long a password must be, what kind of characters a password should contain and how frequently it must be changed) should be appropriate to the circumstances but not be so difficult that users are tempted to write them down.

### **Password Use Policy**

User passwords are sensitive, confidential organizations information and must not be shared with others. Passwords are the first line of protection against threats to network security, whether threats originate internally or externally.

- Minimum Password Length & complexity

- Wherever the system or application can accommodate, passwords must be a minimum of six characters in length.
- A combination of alphabets, numbers and special characters should be used

- Minimum Password Age

- Password age refers to the time during which a password must be used before a new password can be selected. New password shall not be same as of the previous 7 passwords

- Password Expiration and History Management Policy

- The organizations standard expiration period is 90 days. No user account is set to non-expire.
- Passwords must not be repeated within 5 generations.

- Password Lockout Policy

- Users are locked out of their account after three failed logon attempts. Failed logon attempts are the result of attempting to logon using either a faulty logon ID (user name) or password.

- The lockout period remains in force for 30 minutes and the counter is reset after the 30-minute lockout interval.
- Temporary Passwords
  - First-time computer users of the organization (or those requiring a password reset) are given a temporary password that must be changed immediately after the first login.

### **For All Trading Applications:**

User passwords are sensitive, confidential trading information must not be shared with others. Passwords are the first line of protection against threats to network security, whether threats originate internally or externally.

- Minimum Password Length & complexity
  - Wherever the application can accommodate, passwords must be eight characters in length.
  - The password shall be case sensitive and should contain at least one each of the following
    - characters with no space:
    - Uppercase: A to Z
    - Lowercase: a to z
    - Digit: 0 to 9
    - Non-alphanumeric: Special characters @ # \$ % & \* / \
- Minimum Password Age
  - Password age refers to the time during which a password must be used before a new password can be selected. New password shall not be same as of the previous 7 passwords
- Password Expiration and History Management Policy
  - User shall be compulsorily required to change password after the lapse of 6 days
    - No user account is set to non-expire.
    - Passwords must not be repeated within 7 generations.
  - User shall not be allowed to set the default password as new password and the new password cannot include the user id
- Password Lockout Policy
  - Users are locked out of their account after three failed logon attempts. Failed logon attempts are the result of attempting to logon using either a faulty logon ID (user name) or password.
- Temporary Passwords
  - First-time trading application users (or those requiring a password reset) are given a temporary password that must be changed immediately after the first login.

### **Secure Password Guidelines**

The following guidelines are valid throughout organization to protect information and enhance the security of the network: -



- If accounts or passwords have been compromised, report the incident to IT Support and change all passwords immediately.
- If an administrator requires that you login to a machine or service, use precautions so that password(s) are not witnessed.
- Anyone demanding a password must be reported to IT Support.
- Users shall not choose passwords, which can be easily guessed such as the user's name, car registration number, telephone number, birth date etc.
- All vendor-supplied default passwords (or other alternative access mechanisms) must be changed before any computer or communications system is used for any business activity beyond initial evaluation in a test environment. These standards apply to passwords associated with end-user user IDs, as well as passwords associated with systems administrator and other privileged user IDs.
- Users shall not share their password with anyone, including their reporting supervisors or colleagues.
- Passwords should not be written down or left in a place where unauthorized persons might discover them.
- Passwords shall not be stored unencrypted format in system resources.
- Appropriate procedures shall be put in place for storing and management of administrative passwords for critical information systems.

## **SHARED FOLDERS, PERMISSIONS AND DISK QUOTAS-**

- Shared folders allow groups of staff and representatives to access the same files. Disk quotas restrict the amount of data that one employee can store on a server. There are security and performance implications for both.
- We need to ensure the business has appropriate rules in place so that people can see the data they need for their job, but data is generally secured.
- The ITC has been allocated the job of managing shared folders and granting permission to individuals or groups to see the files in those shared folders.
- Permissions to access shared folders are reviewed regularly and permissions are deleted when they are no longer needed (perhaps because someone changed roles within the business).
- Where appropriate, disk quotas are in place that limit the space that an individuals' files can take up on servers. The business server is not the place for individuals to store large files they have downloaded from the web!
- All business data should be stored on the server where it can be secured, and backed up.

## LEASED LINES, MPLS AND INTERNET CONNECTIONS-

- Network connections like leased lines, MPLS and internet connections are very important in smooth running of business. These provide connectivity to other branch offices, data centers and remote/roaming users.
- Downtime and fluctuations in the connection will impact the business, redundant connections are configured to avoid unexpected production stoppages. Maintenance activities should be planned and communicated to the users with advance notice.
- The ITC is responsible for monitoring speed and bandwidth, configuration of the network equipment and dealing with the service provider about problems with the connection.

## INFORMATION REPORTING-

- a. All software systems utilized by the business must be capable of providing the relevant business and management reports required to effectively manage the business.
- b. Relevant exception reports must be included in all reporting functions to ensure early warnings are provided to management when processes or functions are not meeting expected levels.

## SECURITY-

- We must ensure the security of data, especially confidential and sensitive material collected within our Information Technology systems.
- To this end all staff and representatives are to be issued with appropriate system access that enables them to perform their required tasks and only access to data that is appropriate to their role.
- The use of system passwords, user ids and a hierarchy of access will be implemented wherever possible to support this approach.

### Network Server Security

Access to network services and servers must be controlled to ensure that connected users or computer services do not compromise the security of any other networked services.

### Physical Controls for Network Equipment

All critical servers and communications equipment are located in secure locked rooms. Additional controls such as biometric/numeric password access controls are in place to secure critical or sensitive information. Access to secure areas is strictly controlled and restricted to authorize personnel. Secure areas will be monitored by using CCTV systems at all the times. Visitors or

third parties will not be permitted unsupervised access to secure areas. A separate register should be maintained in the secure areas for recording the entry of the people like vendor, contractors etc. who do not have regular access to the secure areas. Any such entry to the secure areas shall only be provided after making an appropriate entry in the register.

## **Logical Controls for Network Equipment**

### **Protection of Network Servers:**

The following procedures must be followed to the security of the network servers:-

- All servers must be protected using strong passwords, and the passwords must be managed as per the defined Password Policy.
- A server should be dedicated to a single network service, wherever possible. This will simplify configuration, thereby reducing the risk of configuration errors. In some cases however, it may be appropriate to offer more than one service on a single host computer (e.g. DNS, ftp and http services).
- The network services that need to be provided on a server must be identified and documented. All unwanted network services must be disabled or removed. Appropriate CRF are maintained for the same.
- A documented backup and recovery plan for critical servers must be prepared, which should include the steps needed to maintain or restore the network services after various kinds of faults.
- A documented procedure for installing the network operating system must be developed and followed. All critical parameter settings, scripts and configuration files used during installation must be documented.

### **System and Network Logging-**

Network logs would be monitored on a whenever needed basis and incidents of abnormal activity will be reported as an exception and the same will be intimated to ITC. At the OS level, system logs will be reviewed on defined basis and if things are normal and no incident is reported, the logs can be flushed from the system and backed up on the tapes for future reference. On Windows platform, event viewer (System, application and security logs) will be reviewed by the system administrator and all suspected activity reported to ITC. Event Viewer can be flushed at defined time for performance enhancement and events can be backed up on the tapes for future reference.

### **Network Switch Security-**

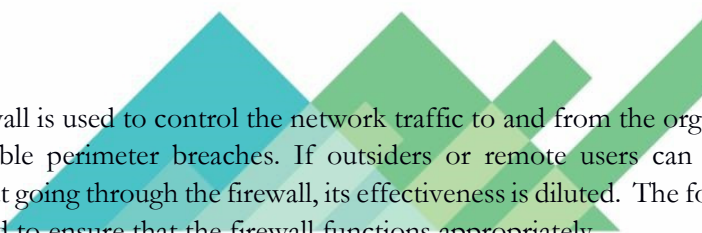
Network Switches direct and control much of the data flowing across computer networks. Using the information presented here, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Control physical access to switch room. Ensure stable version of the IOS/ firmware on each switch. Set timeouts for sessions, Configure privilege levels, Review logs. Configure a banner, if possible, to state that unauthorized access is prohibited. Maintain the switch configuration file offline and limit access.

## **Router Security-**

The following procedures must be adapted to ensure that the routers are properly secured:

- Routers and consoles are housed in a physically secure location.
- All router operating system upgrades from vendors are scanned for viruses before using in the production environment
- All maintenance fixes are applied on the routers during non-peak or off business-hour times
- It is ensured that a backup configuration is available in case the designated change does not work as planned.
- Network router passwords are managed as per the Password Policy. Radius Server is used for Authentication and Accounting the user logins in all the network devices.
- IP Source routing is disabled.
- Routers require a user to enter a user Id and password to gain access to the command prompt.
- Routers have appropriate login banners.
- Copies of the router configuration files shall be restricted to authorize individuals only.
- The router audit logs shall be reviewed regularly

## **Firewall Security**



Company's firewall is used to control the network traffic to and from the organization's network and avoid possible perimeter breaches. If outsiders or remote users can access the internal networks without going through the firewall, its effectiveness is diluted. The following procedures must be followed to ensure that the firewall functions appropriately.

## **Firewall Administration**

For any systems hosting critical applications, or providing access to sensitive or confidential information, internal firewalls or filtering routers must be used to provide strong access control and support for auditing and logging. These controls must be used to segment the internal network to support the access policies developed by the information/data owners. In case, if remote access needs to be provided to service providers, the ITC authorizes such access. Remote access facility to service providers is removed as soon as the job is complete. Physical access to the firewall terminal is limited to authorize people only. Radius Authentication is used for the same. The firewall administrator evaluates each new release of the firewall software to determine if an upgrade is required. Before an upgrade of any firewall component, the firewall administrator confirms with the vendor that an upgrade is mandatory. All security patches recommended by the firewall vendor are implemented in a timely manner.

**Firewall Logs:** The firewall is configured to log all events. Firewall logs are reviewed on whenever needed basis.

**Firewall Backup:** The firewall (systems software, configuration data, database files, etc.) is backed up and a copy of current configuration / last configuration is available on a Central Storage Server which has appropriate access controls applied on the configuration files.

### **Remote Access Security-**

The following procedures must be followed to secure IT systems of the organization when they are accessed remotely. User Authentication for Remote Access

- Firewall is used to separate the organization's network from an external network or a standalone network.
- Firewall is used to protect from all incoming network connections
- External parties are not allowed to connect to the organization's internal network.

### **Modem Security**

Dialing in and dialing out via modems allows users to gain remote access to the network and services respectively. Users are prohibited to setup a dial in modem within organization's internal network

### **Login Banner**

The login banner is displayed at login to all individuals gaining access either intentionally or unintentionally to any system. It advises users that the system is for authorized personnel only and its use may be monitored. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process. The warning banner does not include any system or application identifiers like the type of host hardware or operating system present on the host, information about the organization, the network configuration or other internal matters, which may provide valuable information to a would-be intruder.

### **Clock Synchronization**

System clocks are synchronized regularly especially between the organization's various processing platforms. This allows for generating time-based audit trails.

## **DATA BACKUP AND RETRIEVAL, AUDIT TRAILS-**

The following data backup and retrieval processes are to be implemented and reviewed for effectiveness on a regular basis by the ITC: -

- At the end of each day a backup process to a stable data storage facility is to be performed, involving all business data held on our server(s).
- In an ideal situation there will be backups available for the last 5 years in multiple locations to prevent data loss.
- Where significant software or hardware installations are planned a full back up process and restore test is to be implemented prior to the installation. These backups are to be kept always for the future use.
- The backup data created at month end must be retained at a minimum until the successful completion of the next months back up process.

- All back up storage processes must include clear identification of the date of the back up to facilitate effective and speedy restore processes.
- A comprehensive test of the backup and restore facilities is to be conducted on a quarterly basis or as detailed in the Business Plan.
- A review of data storage on the network should be conducted on a quarterly basis to ensure all business data is being stored on central location and not on individual server(s).
- Any ongoing or consistent problems encountered with either Back Up or Restore processes must be actioned and resolved as a matter of absolute urgency.

### **Trading Applications Backup**

Full backups are performed on all trading day evening for list of files like Orders, Trades, Positions, Risk and User management, Account etc. from trading terminals. Full back up is performed on all trading day evening during EoD for database.

### **Archives**

Trading Application data

Archives are made at the end of every financial year in March and kept for at least 5 **years** for data.

Trading System is stored all the activities in to their database with the IP address from where it is accessed with date and time. Mainly following details are stored in to database:

- ➤ User activities logs

- Alert logs,
- Unique order number generation details (by the system for each order)
- Transaction logs
- Trade Logs
- Order Logs
- Application Logs
- Database Logs

Based on this details IT team can able to generate Audit trail details of last 5 years. All these details are accessible only through valid user-id & password.

### **Non-Trading-**

Archives are made at the end of every financial year in March and kept for at least 3 years for data.

### **Restoration Process**

Trading database restoration will be performed once in a month and logs will be maintained for successful restoration. Other application restoration takes place once in a 3 to 6 months and logs for the same is also maintained. User data restoration will take place as an when request comes from user with appropriate approval.

# CYBER SECURITY INCIDENT RESPONSE PLAN

## OVERVIEW

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan documents how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan defines areas of responsibility and establishes procedures for handling various security incidents.

## PURPOSE

This policy is designed to protect the organizational resources against intrusion and minimize any disruption or damage that an intrusion causes.

## INCIDENT RESPONSE GOALS

- Verify that an incident occurred.
- Maintain or Restore Business Continuity.
- Reduce the incident impact.
- Determine how the attack happened.
- Prevent future attacks or incidents.
- Improve security and incident response.
- Prosecute illegal activity.
- Keep management informed of the situation and response.

## INCIDENT DEFINITION

An incident is any one or more of the following:

- Loss of information confidentiality (data theft)
- Compromise of information integrity (damage to data or unauthorized modification).
- Theft of physical IT asset including computers, storage devices, printers, etc.
- Damage to physical IT assets including computers, storage devices, printers, etc.
- Denial of service.
- Misuse of services, information, or assets.
- Infection of systems by unauthorized or hostile software such as a virus.
- An attempt at unauthorized access.
- Unauthorized changes to organizational hardware, software, or configuration.
- Reports of unusual system behavior.
- Responses to intrusion detection alarms.

## INCIDENT RESPONSIBILITY



The Information Technology Co-Ordinator (ITC) is the primary person for ensuring an appropriate response is made once an incident has been identified. In the absence of the ITC, the responsibility falls to the Responsible Manager(s) of the business.

## **INCIDENT DISCOVERY**

This occurs when someone discovers something not right or suspicious. This may be from any of several sources:

- Helpdesk
- Intrusion detection system
- A system administrator
- A firewall administrator
- A monitoring team
- A manager
- An outside source

## **INCIDENT NOTIFICATION**

The ITC is to be immediately informed of any incident. Our default position is that any incident reported should be assumed to be a real threat to our business operations and managed accordingly until such time it is proven to be benign. The ITC should immediately contact the Responsible Manager(s) and the management of all areas potentially impacted by the incident are also to be immediately advised of the situation.

## **RESPONSE STRATEGY**

In deciding the response required once an incident is reported the following factors need to be considered:

- Is the response urgent?
- Can the incident be quickly contained?
- Will the response alert the attacker and do we care?

## **CONTAINMENT**

Take action to prevent further intrusion or damage and remove the cause of the problem. This may involve:

- Disconnecting the affected system(s).
- Changing Passwords.
- Blocking some ports or connections from some IP addresses.
- Taking down subnets, servers etc.

## **PREVENTION OF RE-INFECTION**

To prevent subsequent re-infection, we need to know how the intrusion happened. We need to determine the source of the intrusion whether it was email, inadequate training, attack through



a port, attack through an unneeded service, attack due to un-patched system or application. Take steps to prevent an immediate re-infection which may include one or more of:

- Close a port on a firewall
- Patch the affected system
- Shut down the infected system until it can be re-installed other steps that may be required include:
- Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
- Change email settings to prevent a file attachment type from being allowed through the email system.
- Plan for some user training.
- Disable unused services on the affected system.

## **RESTORE AFFECTED SYSTEMS**

Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following:

- Re-install the affected system(s) from scratch and restore data from backups if necessary.
- Make users change passwords if passwords may have been sniffed.
- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real time virus protection and intrusion detection is running.
- Be sure the system is logging the correct items.

## **CYBER SECURITY & CYBER RESILIENCE FRAMEWORK**

### **i) Cyber Security Exercises**

Cyber security exercise is a confidence building and learning activity based on simulated cyber security incident scenarios that resemble occurrence of a cyber security crisis. Cyber Security exercises are intended to be a collaborative and coordinated exercise between CERT-In, Sectoral CERTs and key organizations operating in Indian cyberspace. The cybersecurity exercises enable the participating organizations to evaluate their preparedness to deal with cyber crisis situations. In addition, cyber security exercises would also help in;

Identifying preparedness gaps

Addressing gaps by improving processes, communication and information sharing

Enhancing response to cyber incidents

Reducing cyber risk Create awareness among the organizations besides imparting training and education for responding to cyber security incidents.

Install genuine and updated software to strengthen your online safety and security.

## **ii) Reporting of a Security Incident**

A computer security incident is any adverse event whereby some aspect of a computer system is threatened viz. loss of confidentiality, disruption of data or system integrity, denial of service availability.

Any organization or corporate using computer systems and networks may be confronted with security breaches or computer security incidents.

By reporting such computer security incidents to CERT-In the System Administrators and users will receive technical assistance in resolving these incidents. This will also help the CERT-In to correlate the incidents thus reported and analyses them; draw inferences; disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents in future.

## **iii) Reporting of an incident**

System Administrators can report an adverse activity or unwanted behavior which they may feel as an incident to CERT-In. They may use the following channels to report the incident.

E-mail : [incident@cert-in.org.in](mailto:incident@cert-in.org.in)

Helpdesk: +91-1800-11-4949

Fax: +91-1800-11-6969

## **iv) Contents of Incident Report**

The following information (as much as possible) may be given while reporting the incident.

- Time of occurrence of the incident
- Information regarding affected system/network
- Symptoms observed
- Relevant technical information such as security systems deployed, actions taken to mitigate the damage etc.

For details please refer the incident reporting form available on <https://www.cert-in.org.in/>

## **v) Verification**

CERT-In will verify the authenticity of the report.

## **vi) Triage:**

CERT-In will then analyses the information provided by the reporting authority and identify the existence of an incident. In case it is found that an incident has occurred, a tracking number will be assigned to the incident. Accordingly, the report will be acknowledged and

the reporting authority will be informed of the assigned tracking number. CERT-In will designate a team as needed.

### **Incident Response:**

The designated team will assist the concerned System Administrator in following broad aspects of incident handling:

- Identification: to determine whether an incident has occurred, if so, analyzing the nature of such incident, identification and protection of evidence and reporting of the same.
- Containment: to limit the scope of the incident quickly and minimize the damage
- Eradication: to remove the cause of the incident
- Recovery: taking steps to restore normal operation

CERT-In will provide support to the System Administrators in identification, containment, eradication, and recovery during the incident handling in the form of advice. CERT-In will not physically deploy or send any member for attending the incident response activity at the site of occurrence. The priority of assisting in responding to the incidents will be decided by CERT-In keeping in view the severity of incident and availability of resources.

### **Compliance as per SEBI/Exchange Circulars;** (Reference NSE Circular 59/2022 dated 23.08.2022)

- The Company shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Members, whose systems have been identified as “Protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC
- The Designated Officer of the Company (appointed in terms of para 6 of the SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events, all Cyberattacks, threats, cyber-incidents and breaches experienced by Members to NSE (in manner specified by NSE) & SEBI (on the dedicated email ID sbdp-cyberincidents@sebi.gov.in) within 6 hours of noticing / detecting such incidents or being brought to the notice about such incidents as well as submit the quarterly reports containing the information on cyber-attacks, threats, cyber incidents and breaches experienced by Stock Brokers and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges / Depositories and SEBI shall be submitted to Stock Exchanges within 15 days after the end of the respective quarter in the manner as specified by NSE from time to time.
- “Stock Brokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stock Brokers / Depository Participants are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be

submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity...”

VAPT shall be carried out and completed during the period September to November of every financial year and the final report on said VAPT shall be required to be submitted to the Stock Exchanges within one month from the date of completion of VAPT after approval from Technology Committee of respective Stock Brokers.

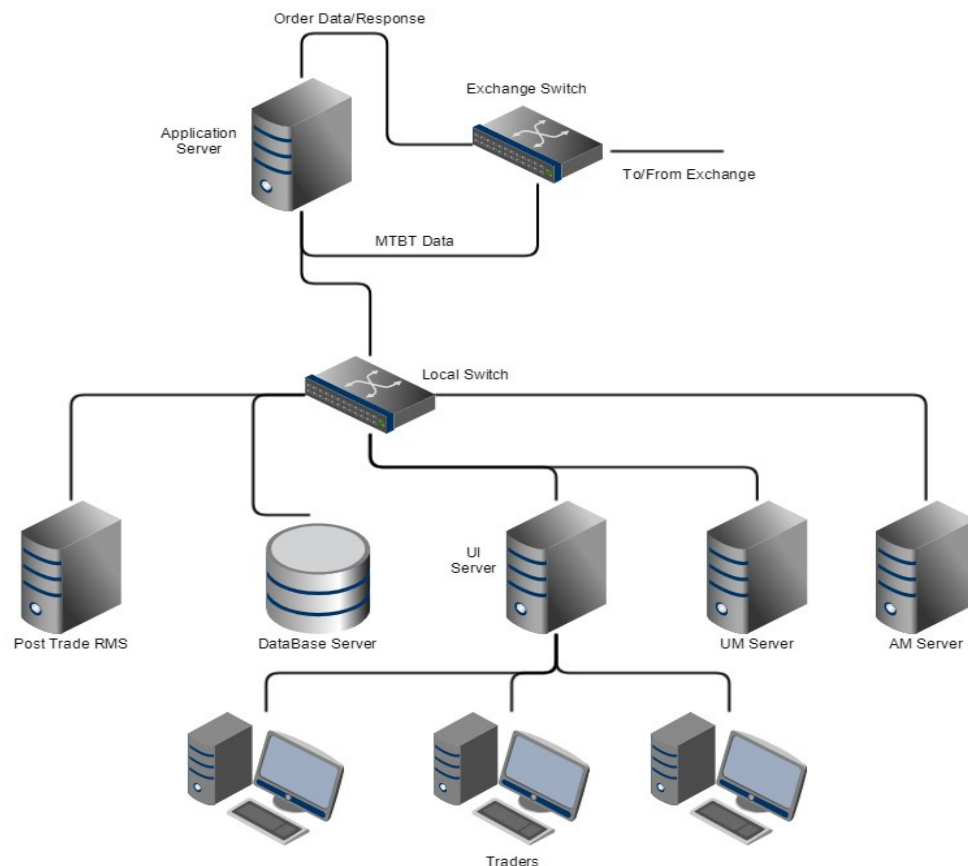
## System Architecture & Development Guidelines

### I) Introduction

This document conveys the informational content of the elements consisting of a system, the relationships among those elements, and the rules governing those relationships. The architectural components and set of relationships between these components that an architecture description may consist of hardware, software, documentation, facilities, manual procedures, or roles played by organizations or people.

A system architecture primarily concentrates on the internal interfaces among the system's components or subsystems, and on the interface(s) between the system and its external environment, especially the user.

#### ii) System Diagram –



### iii) Components of the system –

#### a) Network

Trading network consists of switches and physical links to the servers being used in the trading system. Well planned and designed network is necessary for seamless trading from co-location.

Network involves following components -

- **Exchange Switch**

Main responsibility of this switch is to establish communication channel between exchange and servers in co-location. Receiving feeds and sending orders are managed through this switch. Configuration guidelines are provided by the exchange and it's been followed while configuring the switch.

- **Local Switch**

Connectivity to the servers from member office and communication in-between the systems installed in co-location are managed through this switch.

- **MPLS**

Multiple MPLS links have been installed for uninterrupted connectivity from member offices to co-location facility provided by NSE. The business-critical servers such as Application server, Database server, UM (user management) server, RMS server, monitoring server etc. are installed in the co-location for smooth trading operations. Connectivity downtime to any of the server may impact business; hence multiple MPLS links provided by multiple ISPs have been installed for the redundancy.

- **Application Server**

ALGO trading software runs on this server. Specification of the server depends on the resource utilization of the software being running on it. We use production grade servers with latest hardware available in the industry, whenever there is upgrade available in market hardware components are upgraded if needed.

All the application servers should have well established physical link with exchange switch. Software running on these servers establishes connectivity with exchange through exchange switch and performs receiving feed; computation based on the user input and send the orders to the exchange.

**The approved in-house software undergoes the following steps from ideation to release through Software Development Lifecycle (SDLC):**

- **Requirement Gathering** - A preliminary discussion with various stakeholders is undertaken to understand the basic capabilities required from the system. This is followed by detailed discussions on individual features within the development team with back and forth with various stakeholders to flush out the design and implementation details.
- **Code development** - The requirements are then implemented into the software and exhaustive unit tests are added to ensure the code is tested at the lowest possible level.

- **Code Review** - The code is then reviewed by other members of the team, while a Continuous Integration system ensures that all existing and new tests added continue to pass. Only after this step is the code allowed to merge into the main code line.

**Release Testing** - Multiple changes that form an incremental release are taken and tested individually (automated/manual testing) to ensure there are no regressions in the software. In addition to automated Unit tests and Regression tests, testing is carried out on local machines (Simulator), On Exchange Test Market, Paper Trading (Using live market data), Zero limit testing (Firing orders to exchange) before finally putting the system into Live Trading.

**Change Management:** - All code repositories for the software are hosted on an internally managed central server. Open-source Change Management software called Phabricator is deployed on these servers to help during the various steps of the SDLC.

- Phriction - Access controlled wiki to document features and or processes.
- Diffusion – Access (view/clone/update) controlled Git backed code repositories.
- Maniquest - Task Planning and assignment.
- Differential - Change requests and Code review work flow management.

**M/s Mathisys Advisors LLP**, follow a release branching strategy in Git, i.e. every major Release is maintained on a different branch, with master being the long term development branch. The history of the changes that have been made in the software is available in the git log with each commit linked to the differential that was used for code review for the same.

## **RMS Server**

RMS Server takes care of the RMS operation needed for risk free trading to happen. RMS software is hosted on this server and does the following functions -

There are 2 major operations in RMS:

- Managing positions,
- Validating order requests i.e., checking whether an order can be sent or not based on limits and positions.

Main Components of RMS:

- Portfolio
- Portfolio Manager
- State Node
- RMS Updater
- Order Response Translator
- Order Validator

- **Database Server:** Database software like My SQL is installed on this server to store the various data in an organized format. Trading software is provided with the interface to the database server to fetch and to store configuration, user inputs and real-time trade transactions.

There are multiple database servers to maintain the data generated from different applications like trading software, monitoring software, RMS software, User management system etc. All the data stored in this server is crucial for the business so necessary configurations are in place to protect and maintain data integrity.

- **User management System:** User management system is built to manage the end-user's aka Traders who login to the system on daily basis. Following are the functions provided by this server -

- User creation
- User deletion
- Disabling and enabling users
- Password validation
- Reset passwords

- **Trader work stations:** Trader work station is the front-end provided to the end user for trading in the stock market. TWS can be opened by an authorized trader from his work location over the network. A trader can view and perform all the trading related operations, following are the features available on TWS

- Market watch
- Order entry
- Order modifications
- Order cancellation
- Order book
- Trade book
- Net positions
- Square off-positions

## **Development Process**

Key principles:

- Break features/tasks into smaller logical pieces. Each chunk should be something that can be completed in couple of hours to a day.
- Commit often and get the code reviewed as soon as possible. It is good to sketch out a skeleton implementation very quickly and get feedback on the approach before working on the details.
- Any development / investigation work has to have a Phabricator task associated with it. Create one if it doesn't exist. The task description should contain an overview of problem being addressed. Add additional comments as you work on the task - summary of discussions / decisions, alternate approaches tried anything that doesn't go directly into the code repo should be added as comments to the task.



- Every commit must be associated with functional unit tests covering the changes that are being made. For a new feature all the positive flows and the key negative flows must be covered. For a bug start by writing a unit test to reproduce the issue before attempting a fix. Make sure all existing test cases pass, don't comment out / disable any existing tests.
- Implement micro benchmarks for performance critical parts of the code. These should be automated and repeatable.
- New code should blend into existing code. Follow all the coding guidelines, idioms, choice of data structures - both explicitly stated and ones that are implicitly followed. If you find instances where the current approach is wrong or sub optimal discuss with the team and get an agreement for doing things differently. Also plan to fix existing code.
- Create feature branches for large features which need to be tested thoroughly before getting merge to master.

### **Coding guidelines:**

We are following the Google C++ Style guide with a few minor exceptions outlined below. Browse through the document and become familiar with it. Automated scripts are provided to reformat code, check violations.

<https://google.github.io/styleguide/cppguide.html>

#### **Exceptions:**

- Use `#pragma once` - instead of include guards
- Member variable names should start with `m_` instead of prefixing with `_`

For Python we are following Google Python Style guide without any exceptions.  
<https://google.github.io/styleguide/pyguide.html>

### **Code work flow:**

- One time setup - this sets up `~/ .arcc` on a new machine. No need if you already have this file. Follow the steps printed on the output. `#arc install-certificate`
- Start working on the task
- `#arc feature {feature name}` (i.e. `ticket_no_brief_description_of_change`)
- Keep Committing the code. And run
- `#arc lint`
- Push the code for review and write appropriate summary and test plan
- `#arc diff`
- Get the code reviewed and make changes as per suggestion.
- Once the revision is done.
- `#arc land {feature name} --keep-branch`
- Run `"arc which"` at any point to get hints/explanation on how to proceed.

## **ENFORCEMENT**

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or legal action as appropriate, or both. No provision of this policy will alter the at-will nature of the employment relationship at the organization.



## **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 to the followings:

- To attend the cyber safety and training programs as conducted by the company from time to time.
- To endure installation, usage, and regular update of antivirus and antispyware software on the computers 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.
- Make backup copies of important business data and information.
- Control physical access to your computers and network components.
- Keep your Wi-Fi network secured and hidden.
- To adhere to limited employee access to data and information and limited authority to install the software.
- Regularly change passwords.
- Do not use or attach unauthorized devices.
- Do not try to open restricted domains.
- Avoid saving your personal information on a computer or any financial data on any unauthentic website.
- To get your computer regularly scanned with anti-virus software.
- Do not release sensitive data of the organization.

## **PERIODIC REVIEW AND ACCEPTANCE**

This policy has duly placed and duly approved and reviewed by the board of the Mathisys Advisors LLP, further board has decided to have an annual periodic review of the same or as and when feel necessary as per the guideline issued by regulatory bodies from time to time. The company shall arrange to have its systems audited on an annual basis by a CERT-IN empaneled auditor or an independent CISA / CISM qualified auditor to check compliance with the above areas and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board/ Committee / any committee thereof within three months of the end of the financial year, Furthermore, the company shall also get certified from empaneled auditor for Vulnerability Assessment and Penetration Testing (VA-PT) as suggested by SEBI on yearly basis.

**For M/s Mathisys Advisors LLP**

Policy maker: Ms. Ruchi Chandna, (Compliance officer)

Policy Checker: Nihit Gupta, (Designated Partner)

Last review of policy: February 11, 2023.

**Policy Review Period: Annual Policy version: 1.1**