JSEL Securities Ltd.

Member of BSE Cash Segment
Clearing No. 287

Different Policies

Version : 4.0

Principal Officer : Mr. Shobhit Rawat
Compliance Officer : Mr. Alok Nigam
Designated Director : Mr. Alok Nigam
Approved By Board Dated : 05/12/2023

Policy Regarding Prefunded Instruments

It’s a Policy of the Company for the acceptance of Prefunded Instruments. This policy is Subject to the rules and regulations of the Exchange from time to time.

Title: Acceptance of Prefunded Instrument for trades on Exchange.

Coverage: All Sub Brokers Branches of the Company wherever trading terminals / WEB terminals are Located.

Scope: Acceptance of Prefunded Instruments like Demand Draft/Payorder /Bank Guarantees from a client against Payin Obligation/ Margin.

Policy : As per company policy, we do not accept any prefunded instruments and cash from the clients.

POLICY ON SETTING OF LIMITS FOR TERMINALS

Objective: To pre- define limits for each terminal and monitor the same on a continuous basis as per the rules and regulations of the Exchange.

Background: Trading Terminals are allotted to Members by exchanges. These terminals enable members to place, modify and execute orders on behalf of clients. There may be instances where due to punching error unusual orders may be placed at high prices which might lead to execution of unrealistic orders or orders being executed at unrealistic prices. In cases where the order/price of such orders is high, it might lead to huge losses to broker. In order to avoid such a situation it is imperative that certain limits are prescribed for each terminal allotted to member broker.

Scope of the Policy: This policy covers the procedure and checks in place for allotting limits to each TWS Terminals.

Defining of Limits: The following limits shall be defined for each terminal:

1. Quantity Limit for each order
2. Value Limit for each order
3. Limit on each TWS Terminal allotted to Sub Brokers

Procedure for setting of Limits: We define limits for each TWS terminal provided by BSE and monitor the same on a daily basis. This policy covers the procedure and checks in place for allotting limits to each Sub broker terminal according to their deposits to the company after deducting Margin and previous day Exposure. Company also have a check on Quantity Limit for each order and Value Limit for each order for every terminal.

Policy on Client Code Modification and error Code Policy

The main objective of the company to framed a policy for modification of client code for post trade execution and takes the report on such modification of client codes. Further educate the Sub Brokers and create awareness among them about this policy.

Brief criteria about Client code Modification

Client code modification means modification of client code after the execution of trade. The stock exchange provides a facility to modify the client code to rectify an error. The modification of client code is to be done only in exceptional cases and not in routine case.

Details about Genuine error

The following trades shall be modify/ allowed to be modify, shall be treated as genuine error .

1. Punching error / typing error of client codes due to any genuine error or mistake in order entry, while punching the order by any of Sub Broker.
2. Trade entered for wrong client due to any miscommunication from the client /authorized representative of the client.
3. Family Code (spouse, dependent parents, dependent children and HUF)

Reporting System

Client code modification issues should be reported to the Key Personnel's and can be done only after getting approval from authorized person.

RISK MANAGEMENT POLICY

M/s JSEL Securities Ltd. a Trading Member of BSE. As per the requirement of Exchange & SEBI, Company has designed a “Risk Management Policy” for extending trading facility to its clients and in the respective segments of exchanges.

RMS works on the following concepts:

1. Cash: The clear balance available in the customer’s ledger account in our books.

2. Margin: Provided by the customer in the form of cash, FDR, Securities (accepted by the exchange for margin purpose).

3. Exposure: The aggregate of the customer’s obligations arising out of buy + sell trades awaiting settlement in the cash segment and profit/ loss amounts + Margins that are yet to be settled on the closed Positions.

4. Exposure multiple: The number of times that exposure is allowed on the underlying margin sales on the cash segment would have to be made either on the availability of cash margin or on the availability of the stocks in our margin account.

5. Stock qualifying for margin in cash segment transactions: Securities in the approved list of Stock Exchange as per BSE/SEBI guidelines.

6. Total Deposit: The aggregate of client deposit available with us in the form of cash, Shares (After Applicable Hair Cut) and FDR(if any).

Risk based approach:-

Classification of both the new and existing clients into high, medium or low risk category depending on parameters such as the customer’s background, type of business relationship, transactions etc. Application of each of the client’s due diligence measures on a risk sensitive basis and adoption of an enhanced customer due diligence process for high risk categories of customers and vice-á-versa.

Limit Setting:- Limits shall be monitored on daily basis, taking following criteria’s: Turnover, Exposure, past trends, Deposit/Collateral.

Margins:- Margin must be collected on all Orders in BSE Cash Segment and after as per Margin file of BSE.

Pay-in of Fund & Stock:- Third party pay-in of securities & fund will not be accepted. Same way pay out of shares and fund will be directly done to client account only. No securities belonging to one client be used/transferred for Own purpose or for other client.

Further in addition to above as per SEBI circular no. CIR/HO/MRDSD/DOP/CIR/P/2019/75 dated June 20, 2019 related to Handling of Clients' Securities by Trading Members/Clearing Members, following important changes included w.e.f October 01, 2019:
Securities purchased by client shall be transferred to client's demat account within one working day of the pay-out subject to clear credit balance in clients' trading account (Capital Segment).
With regard to securities that have not been paid for in full by client (unpaid securities), full/partial securities shall be transferred to a separate client account titled as "Client Unpaid Securities Account(CUSA)". The securities kept in the "Client Unpaid Securities Account" shall be transferred to client's demat account upon fulfilment of funds obligation within five trading days from the pay-out date otherwise the same will be disposed off in the market by JSEL. However, JSEL may at its sole discretion, transfer all or part of the securities from Pool/Client Unpaid Securities Account to client's demat account even there is a debit balance in client account subject to availability of sufficient collaterals. If unpaid securities of the client are disposed off by JSEL as per SEBI circular, then the client is not allowed to purchase the same securities on the same day unless the debit balance is cleared by the client.

INVESTOR COMPLAINT REDRESSAL MECHANISM

1. The company has a designated investor grievances email id jselsecurities@yahoo.com on which the client or investor can make a complaint.

2. An Investor / client can make a written complaint through letter also.

3. The Company maintains investor grievance register in which full detail of every written complaint shall entered.

4. Designated person shall login the designated investor grievances email id on daily basis to look after the investor complaint whether new complaint has been lodged or not.

5. Compliance officer will obtain all information available on the compliant which is considered necessary for a proper investigation. Look into all the necessary information and resolve as soon as possible.

6. There is standing policy of the company to resolve the investor compliant as soon as possible of the receipt of the same expect the complicated case.

7. A serious compliant (where the written response does not settle the issue) must be referred to the Directors of the company.

8. The Designated person of the company shall review the investor compliant register on weekly basis to find out whether complaint has been resolved within time.

Code of internal procedures and conduct for Prevention of Insider Trading

Principal Officer:
Company appointed Ms. Shobhit Rawat as principal officer under the provisions of Insider Trading.

The Principal Officer will ensure that:

The Insider Trading Prevention program is communicated and implanted effectively, monitoring adherence to the rules for the preservation of “Price Sensitive Information”

Monitoring of trades and the implementation of the code of conduct.

Regular updation regarding any changes/ additions/ modifications in PMLA provisions.

Employees/directors shall maintain the confidentiality of all Price Sensitive Information.

Employees/directors must not pass on such information directly or indirectly by way of making a recommendation for the purchase or sale of securities.

Policy on Circulation of Unauthenticated News

Prohibition on circulation of unauthenticated News:

To Protect Investors to Stop Unauthenticated News Circulation by the Company's Employees/ and by company Infrastructure. All SEBI registered market intermediaries are required to have proper internal code of conduct to govern the conduct of its Employees. In view of same, JSEL Securities Ltd. implements code of conduct for communicating through various modes of communication. Company Directors/ Officers / Employees are prohibited from:

1. Circulation of unauthenticated news related to various Scrips in blogs/chat forums/e-mail etc.

2. Encouraging or circulating rumors or unverified information obtained from client, industry, any trade or any other sources without verification.

3. Either forwarding any market related news received in their official mail/personal mail/blog or in any other manner except after the same has been seen and approved by the Compliance Officer.

If an employee fails to do so, he/she shall be deemed to have violated the various provisions contained in SEBI Act/Rules/Regulations etc. and shall be liable for disciplinary action.

This code can be modified/amended/altered as required from time to time in compliance of the relevant provisions/regulations in this regard .

Policy regarding treatment of Inactive/Dormant Account

The objective of the policy is to appropriately deal with the Inactive/dormant clients, where clients have not traded for more than 12 continuous months.
The policy is also applicable for accounts which have been marked inactive on account of Rules, Bye laws, circulars and guidelines issued by Sebi, Exchanges and Internal Risk Management Policies.
SEBI vide circular no. dated December 3, 2009 and National Stock Exchange vide circular no. NSE/INSP/13606 dated December 3, 2009 directed that a policy be framed by stock brokers to deal with the inactive/dormant accounts.

Policy:

Procedure to handle Inactive/dormant accounts:

If there is no transaction (buy / sell) entered into by the account holder for more than 12 continuous months, the account will be marked as “INACTIVE/DORMANT".

All the accounts marked as “INACTIVE/DORMANT” needs to be monitored carefully in order to avoid unauthorized transactions in the account. If the client wants to make the account “ACTIVE” after 12 continuous months or after providing the required documents supporting the the client needs to submit a request to reactivate his/her account. In case there is any change in the information such as; address, mobile number, email id, bank/demat account, financial disclosure provided in KYC at the time of registration as client, the same has to be submitted along with the request. After proper verification of the updated / revised details and approval from the compliance officer / or concerned department in-charge of registration of clients, the account can be made “ACTIVE” and transaction can take place.

Process for reactivation of Inactive / dormant account which are inactive for 11 continuous months:

The Client can follow any of the below processes:

Client can give the duly signed request in writing to trading member, Address Proof – such as Aadhar Card, Electricity Bill, Passport Copy. Identity Proof such as Aadhar Card , Passport Copy, Pan Card.

Review Policy:
This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change on account of business needs and Risk Management policy.
The policy may be reviewed by the Office In charge and place the changes in policy before the Board.

Policy on NISM Series VII-Securities Operation & Risk Management (SORM)

Brief SEBI issued Notification no. LAD-NRO/GN/2010-11/21/29390 dated December 10, 2010 according to which, following categories of associated persons associated with a registered stock broker/trading member/clearing member in any recognized stock exchanges, who are involved in, or deal with any of the following:

a. Assets or Funds of investors or clients
b. Redressal of investor grievances
c. Internal control or risk management
d. Activities having a bearing on operational risk

shall obtain the valid certification of NISM Series VII - Securities Operation and Risk Management (SORM) within two years from the date of such notification. Simultaneously, whenever the company employs any associated person specified as mentioned above, the said associated person shall obtain valid certification of NISM Series VII – Securities Operation and Risk Management (SORM) within one year from the date of his / her employment.

Definition - Associated Person

“Associated Person” means a principal or employee of an intermediary or an agent or distributor or other natural person engaged in the securities business and includes an employee of a foreign institutional investor or a foreign venture capital investor working in India.

Exemption

Associated persons handling the basic clerical / elementary functions in the aforesaid specified areas shall be exempted from obtaining the certification of NISM Series VII – Securities Operation and Risk Management (SORM). For this purpose, the company considers following activities as basic elementary level / clerical level.

Internal Control or Risk Management

1. Inwarding or collateral’s / Cheques
2. Person performing market entries
3. Maker entry in the database
4. Preparing of MIS
5. Sending of letters / reports to clients, Exchanges, SEBI
6. Attending Calls, etc.

Redressal of Investor Grievances

1. Inwarding of complaints
2. Seeking documents from clients
3. Person performing maker entries
4. Maker entry in the database
5. Sending of letters / reports to clients, Exchanges, SEBI updation, data entry, uploading on SCORES
8. Attending calls, etc

Activities having a being on operational risk and dealing with assets of funds of investors of clients

1. Person performing maker entries
2. Maker entry in the database
3. Preparing of MIS
4. Generating of reports, Files
5. Sending of letters / reports to clients, Exchanges, SEBI
6. Attending calls, etc

However, any of the work (as stated herein above) being performed by such persons, obtaining, NISMSORM Certification shall be optional provided that they are supervised by his / her supervisor who shall have to obtain / continue to have NISM – SORM Certification or such other prescribed certification at all times. In case of any query, employees are requested to obtain clarification from the Compliance Officer of the Company

BACKUP POLICY

A backup policy is : “Backup my files every “X” period at NN hours, and put the backed up files on a disk, FTP server or a zip archive.” All employees are responsible for taking appropriate steps, as outlined below, for effective backup policy.

1) Backup should be taken on regular basis because you can’t restore what is not backed
2) Have daily back-up of data at EOD on at least two nodes and external Hard disk, Do EOD back-ups on different nodes for different days of the week to ensure 3-4 back-ups are readily available in case necessity arises.
3) Have multiple backups of data on different backup media. There is a chance that backup media will be corrupted or lost too.
4) Always store at least one complete backup off-site to protect yourself against fire, theft or natural disaster, periodically review the off-site back-up data for updation as well as to its being restorable.
5) Take care of your backup media, which can easily be damaged by the environment.
6) Periodically verify your backups are working properly.

.

7) Separate the most important and used files from the little used files. This will allow you to restore most important files with minimum time requirements and continue your work. The above backup policy must be strictly adhered to by the employees responsible for taking backups.

PASSWORD POLICY

Authentication is the process of identifying users in a manner which makes it difficult for one user to impersonate another. Passwords are an important aspect of computer security. They are the front line of protection for user data. A poorly chosen password may result in the compromise of company's entire corporate network. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. All employees are responsible for taking appropriate steps, as outlined below, to select and secure their passwords.
Password Should be Minimum 6 and Maximum 12 character long having combination of Alphabet, digit and special character.

1) All system level passwords must be changed frequently or at least on a quarterly basis.

2) Passwords must not be inserted into email messages or other forms of electronic Communication.

3) Password must not be revealed over the phone to anyone.

4) Password must not be shared with family members.

5) Password must not be revealed to co-workers while on vacation.

6) Password must not be written and stored anywhere in the office.

7) Password must not be stored in a file on any computer system without encryption.

INFORMATION SECURITY POLICY

Introduction We have introduced the physical controls at server room by not permitting any unauthorized entry physically. No visitor is allowed in this area without prior approval and they are not allowed to carry any laptops, pen drives, floppies, cds etc., inside the secured areas. All employees are not allowed to carry any information in any form from the office while leaving the office. No direct access to Internet is provided to anyone other than authorized persons. All the computers are controlled, their activities are frequently viewed by senior officials time and again to ensure that no pilferage of any sensitive information. No third party vendors, contractors are permitted in restricted zone. Any meetings with this person if required are held at non secured zone office at the front office.

Physical controls of office premises and facilities:

Physical security guard stationed at the entry point guards the office and no unauthorized entry is permitted. Apart from that Biometric locking arrangements are maintained.

Protecting against external environmental risks:

No open or vacant area is left in the office. Photographic video, audio or any recording equipments like cameras in mobile devices are not permitted inside the secured area. Even employees are not allowed to carry their mobile phones with camera to have full proof physical security of sensitive information. We have also ensured to discard all unused or unserviceable equipments, Records, papers not required are destroyed to avoid the unnecessary piling up of unused materials to avoid the dust, fire, explosion, vibration, chemical, electrical damage. Information Security policy and Network Security Policy Purpose The purpose of this policy is to outline acceptable use of computer equipment at Company. These rules are in place to protect the entire Company’s team and Company. In appropriate use expose risks including virus attack, compromise of network system and service and legal issues. Scope This policy covers employees, contractors, consultants and temporaries including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company. Policy

1. The legitimate use of network and reasonable level of privacy is ensured.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

3. This policy recommends that any information that is considered sensitive is encrypted.

4. Regular Audit of network system is done on periodic basis to ensure the Compliance of this policy.

We have introduced the physical controls at server room, back office room by not permitting any unauthorized entry physically. No direct access to Internet is provided to anyone other than authorized persons. All the computers are controlled, their activities are frequently viewed by senior officials time and again to ensure that no pilferage of any sensitive information.

Cyber Security Policy Preface

Rapid technological developments in securities market have highlighted the need for maintaining robust cyber security and cyber resilience framework to protect the integrity of data and guard against breaches of privacy. Since JSEL Securities Ltd. (JSELS), as stock broker and as depository participant, perform significant functions in providing services to holders of securities, it is desirable that ISPL have robust cyber security and cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.

Need of Policy

JSELS is required to Identify, assess and manage the Cyber Risks associated with processes, information, networks and systems. In JSELS, in order to achieve the above target, a need of policy for cyber security arose. Cyber Security Framework and Policy.

1. 'Identify' critical IT assets and risks associated with such assets.
2. 'Protect' assets by deploying suitable controls, tools and measures.
3. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes
4. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.
5. 'Recover' from incident through incident management and other appropriate recovery mechanisms.
6. 'Training and Education' to the staff of JSELS.

To implement the above framework, a Technology Committee is formed comprising of following individuals:

1. Ms. Akshay Gadodia
2. Mr. Alok Nigam, D G M (IT)
3. Mr. Shobhit Rwat, Compliance Officer (Depository), Technology Executive

Mr. Alok Nigam shall also be held as Designated Officer for the purpose of this policy.

Identification:

Mr. Alok Nigam, jointly with Mr. Shobhit Rawat of the company will identify all the critical assets based on their sensitivity and criticality for business operations and shall maintain an Up to Date Inventory of its hardware and systems along with name and ID details of personnel to whom such hardware and systems are issued. He shall also be held responsible to identify the software installed, details of network, data flowchart and connection to the networks. Mr. Alok Nigam alongwith Mr. Shobhit Rawat and external agencies (if required), shall identify the cyber risks that JSELS may face alongwith the likelihood and impact of the same on business of company.

Protection:

No unauthorised person, irrespective of his/her designation, post or rank should have right to access critical systems, confidential data, applications or facilities. Password Policy is made mandatory for all level of data access with sufficient complexity of the Password placed. Any access given shall be for defined period and defined purpose only. JSELS should grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms. The access to the IT systems, applications, databases and networks needs to be sent on mail approved by immediate superior. Any Application offered by JSELS to Customers containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. (referred to as "Application" hereafter) over the Internet should be password protected. A minimum length of 6 characters of complex password shall be enforced across the applications. An attempt to educate the customers shall also be made by team. Two Factor Authentication shall also be implemented across the applications in phased manner. Passwords, security PINs etc shall be stored in encrypted manner in one way hashed encryption using cryptographic hash functions. After Three (3) failed login attempts into Applications, the users account can be set to a "locked" state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the users registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer's registered mobile number, or manually by JSELS after verification of the users identity etc. JSELS shall also ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. JSELS shall formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the critical IT Infrastructure. IT team shall also address deactivation of access of privilege of users who are leaving the organization or whose access privileges have been withdrawn. Physical Security Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees. Physical access to the critical systems should be revoked immediately if the same is no longer required. Perimeter of the critical equipment room (server Room)shall be secured physically and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, etc. where appropriate. Network Security Management Continuous and consistent application of security configuration shall be made to Operating Systems, Databases, Network devices and enterprise mobile device with in the IT environment. The LAN and wireless network networks shall be secured with Firewall and Intruder Controller and continuous monitoring shall be made towards any attempt of unauthorised access to the network. Every individual as well as network connected system shall have an Anti Virus Software with Anti Malware and Anti Ransomware protection. Data Security All the critical data need to be identified and encrypted using strong encryption methodologies, such as masking of critical information, masking of passwords while logging in, encrypted transfer of password to server etc. All the ports, for connecting external storage device or unauthorised USB tokens, of all critical systems as well as network connected systems shall be disabled and log shall be maintained for all the access granted for any given time to any users with specific reason of same. Any authorised access to Printers, Scanner shall be prevented by application of proper access control and restricting the usage to prevent misuse of resources and to avoid transmission of sensitive data. Use of mobile phones shall not be allowed to any employees for dealing with clients as well as any other external parties and any call to clients shall be made using baseline phones having voice logger facility only. Hardening of Hardware and Software Procurement of all the hardware and software shall be done from renowned vendor/supplier only in company sealed packaging and any unauthorised software and hardware shall not be installed on any system, which form part of network. All the test software and hardware shall be installed and tested on designated separate system/network to prevent misuse from such devices and software. Certification of off-the-shelf products IT team shall ensure that all the off-the-shelf products procured for core business activities should bear Indian Common criteria certification of Evaluation Assurance Level 4 provided by STQC. Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls. Patch management Team shall perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems. Team shall also ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner. Disposal of data, systems and storage devices Any disposal of any data, system or storage devices shall be done in closely monitored manner. All the sensitive data, including encrypted system files, shall be removed completely before disposal of any system or storage device. Vulnerability Assessment and Penetration Testing (VAPT) IT Team with the help of IT Experts shall regularly conduct vulnerability assessment to detect security vulnerabilities in the IT environments exposed to the internet. Penetration test shall also be carried out atleastonce in a year In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, IT Team shall report them to the vendors and the exchanges in a timely manner. Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

Monitoring and Detection :

We shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet shall also be monitored for anomalies. Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, we shall implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.

Response and Recovery :

Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident. The response and recovery plan should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes Sharing of Information Quarterly reports containing information on cyber-attacks and threats experienced by our team 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 shall be submitted to Stock Exchanges / Depositories.

Training and Education :

We shall work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines). We shall also conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. The training programs should be reviewed and updated by team to ensure that the contents of the program remain current and relevant.

Systems managed by vendors Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) are managed by vendors and due to which we shall not be able to implement some of the aforementioned guidelines directly, we shall instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self certifications from them to ensure compliance with the policy guidelines. Periodic Audit We shall arrange to have our system audited on periodic basis and shall obtain certification from any independent auditor, capable to do the same.
