POLICY ON CYBER SECURITY AND CYBER RESILIENCE

Introduction

Details on the Profile of the **GRD Securities Limited**

Background

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

In order to protect the integrity of data and guard against breaches of Privacy and to comply with the applicable regulations **GRD Securities Limited** has framed a policy for implementation to meet the objectives.

Date of Implementation of the Circular

Circular shall be effective from April 1, 2019.

It is observed that the level of Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack

Accordingly, the following Policies & Procedures have been put in place: -

Governance

Risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats.

- Identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:
  - 'Identify' critical IT assets and risks associated with such assets.
  - 'Protect' assets by deploying suitable controls, tools and measures.
  - 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes.
  - 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.
  - 'Recover' from incident through incident management and other appropriate recovery mechanisms.

- As a Stock broker trading through APIs based terminal or acting as a depository Participants should refer best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

  - ISO 27001 is an international standard for the establishment, implementation, maintenance, and continual improvement of an Information Security Management System. The standard is a joint effort by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).
  - COBIT 5 is a framework from the Information Systems Audit and Control Association (ISACA) for the management and governance of information technology (IT). ... Achieve strategic goals by using IT assistance. Maintain operational excellence by using technology effectively. Keep IT-related risk at an acceptable level.
  - The main benefit of implementing ISO 27001 is a systemic Information Security Management System that helps with the identification of critical information,

the information security risk assessment of the system, and the implementation of security controls, all of which help to create a secure culture in the organization.

- ISO 27001 is beneficial for the organization in terms of its security.
- The five COBIT 5 principles are:
  - Meeting stakeholder needs
  - Covering the enterprise end to end
  - Applying a single integrated framework
  - Enabling a holistic approach
  - Separating governance from management

- We have designated Mr Lokenath Ghosh 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.
- A reporting procedure has been designed to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
- The Designated officer and the technology committee will periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

Identification

- We have identifiedand classified / designatedcritical assets based on their Sensitivity and criticality for business operations, services and data management. The critical assets include business critical systems, internet facing applications / systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance are classified as critical system. Maintenance of up-to-date inventory of the hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows. Accordingly identify

cyber risks, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

- To this end, XYZ Limited is maintaining up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

Protection

Access controls:

- Any access to systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. To identify the access we have granted access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases.
- Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the critical systems, networks and other computer resources, should be subject to stringent Supervision, monitoring and access restrictions.

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. Access should be revoked immediately if the same is no longer required.
- Office premises should be physically secured and monitored by security guards.

Network Security Management:

- As a Stock Brokers / Depository Participants we have established baseline standards to facilitate Consistent application of security configurations to operating systems, databases, Network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks should be secured within the premises.
- Adequate controls must be deployed to address virus / malware / ransom ware attacks.

Data security:

- Strong encryption methods to be used for identifying and encrypting the critical data. The confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc.

Hardening of Hardware and Software:

- Should deploy hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system. Open ports on networks and systems which are not in use should be blocked.

Application Security in Customer Facing Applications:

- Application security for Customer facing applications offered over the Internet such as IBTs, portals containing sensitive or private information and Back office applications are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. Measures to be taken for applications.

Patch management:

- Patch management procedures should 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.

Testing to be performed on 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.

Disposal of data, systems and storage devices:

- Identify a Policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

Vulnerability Assessment and Penetration Testing (VAPT):

- XYZ Limited willcarry out periodic vulnerability assessment and penetrationtesting (VAPT) which inter-aliaincludes all critical assets and infrastructurecomponents like Servers, Networking systems, Security devices, loadbalancers, other IT systems in order todetect security vulnerabilities in the IT environment andin-depth evaluation of the security posture of thesystem throughsimulations of actual attacks on its systems and networks.
- XYZ Limited will conduct VAPT at least once in a financial year. However, whose systems have been identified as "protected system" byNational Critical Information Infrastructure Protection Centre (NCIIPC),VAPT shall be conducted at leasttwice in a financial year. Further, only CERT-In empanelled organizations are required to engage forconducting VAPT.
- The final report on said VAPT should be submitted toSEBI after approval from Standing Committee on Technology (SCOT), within 1 month of completion of VAPT activity.
- Anygaps/vulnerabilities detected have to be remedied on immediate basisand compliance of closure offindings identified during VAPT shall besubmitted to SEBI within 3 months post the submission of finalVAPTreport to SEBI.In addition, XYZ Limited should also perform vulnerability scanning and conductpenetrationtesting prior to the commissioning of a new system which is acritical system or part of an existing criticalsystem.Systems which are publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct

an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet.

Monitoring and Detection:

- 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 should also be monitored for anomalies.

- Ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, 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 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. Stock Brokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time.

Sharing of Information:

- All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.
- The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stock Brokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.
- The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depository Participants 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 / Depositories within 15 days from the quarter ended June, September, December and March of every year.

Training and Education

- Entities should 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. Where possible, this should be extended to outsourced staff, vendors etc.
- The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Systems managed by vendors, MIIs

- As a Stock Brokers / Depository Participants we have instructed 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

- The periodicity of audit for the purpose of compliance with Cyber Security and Cyber Resilience provisions for depository participants shall be annual.
- The periodicity of audit for the compliance with the provisions of Cyber Security and Cyber Resilience provisions for stock brokers, irrespective of number of terminals and location presence, shall be as under: (Type of stock broker as specified in SEBI circular CIR/MRD/DMS/34/2013 dated November 06, 2013)

  - For Type I - Annual
  - For Type II - Annual
  - For Type III - Half-year.

Advisory regarding Cybersecurity best practices –

- **Roles and Responsibilities of Chief Information Security Officer (CISO)/ Designated Officer** – To define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy.
- **Measures against Phishing attacks/ websites:**
  - We need to proactively monitor the cyberspace to identify phishing websites w.r.tto domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.
  - Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence. Additionally, the advisories issued by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.
- **Patch Management and Vulnerability Assessment and Penetration Testing (VAPT):**
  - All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.
  - Security audit / Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis and in accordance with the Cyber Security and Cyber Resilience circulars of SEBI issued from time to time. The observation/ gaps of VAPT/Security Audit should be resolved as per the timelines prescribed by SEBI.
- **Measures for Data Protection and Data breach:**
  - To prepare detailed incident response plan.
  - Enforce effective data protection, backup, and recovery measures.

- Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data.
- Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.
- Deploy data leakage prevention (DLP) solutions / processes.

- **Log retention -** Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. Advisable to audit that all logs are being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done.
- **Password Policy/ Authentication Mechanisms:**
  - Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex-employees Passwords should not be reused across multiple accounts or list of passwords should not be stored on the system.
  - Enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems.
  - Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.
- **Privilege Management:**
  - Maker-Checker framework should be implemented for modifying the user's right in internal applications.
  - For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) shouldbe implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.
- **Cybersecurity Controls:**
  - Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving

and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

- Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.
- Restrict execution of "PowerShell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
- Utilize host-based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
- Practice of whitelisting of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.

- **Security of Cloud Services:**
  - Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
  - Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.
  - Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.
  - Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
- **Implementation of CERT-In/ CSIRT-Fin Advisories** - The advisories issued by CERT-In should be implemented in letter and spirit by the regulated entities. Additionally, the advisories should be implemented promptly as and when received.
- **Concentration Risk on Outsourced Agencies:**

- It has been observed that single third-party vendors are providing services to multiple REs, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyber-attack, happens at such organizations, the same could have systemic implication due to high concentration risk.
- Thus, there is a need for identification of such organizations and prescribing specific cyber security controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk.
- Further, to consider this concentration risk while outsourcing multiple critical services to the same vendor.

- **Audit and ISO Certification:**
  - SEBI's instructions on external audit by independent auditors empanelled by CERT-In should be complied with in letter and spirit.
  - To go for ISO certification as the same provides a reasonable assurance on the preparedness of the RE with respect to cybersecurity.
  - Due diligence with respect to audit process and tools used for such audit needs to be undertaken to ensure competence and effectiveness of audits.

Principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India:

- Protection of Critical Information Infrastructure (CII) is of paramount concern to governments worldwide. To address this threat, the Government of India has notified the 'National Critical Information Infrastructure Protection Centre' (NCIIPC) as the nodal agencies vide Gazette of India notification on 16th January 2014.

- NCIIPC is driven by its mission to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders with a vision to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country. To achieve this, it is essential to

ensure that relevant security mechanisms are built into Critical Information Infrastructure as key design features.

- The National Security Advisor had in July 2013 released a document listing forty controls and corresponding guiding principles for the protection of CIIs. In view of the dynamic nature of cyberspace and to ensure the continued relevance of these controls, NCIIPC is continuously reassessing these based on ongoing experience as well as feedback from NCII constituents, these controls have been grouped into five sets (or families). While all Controls in a family may not be relevant to a particular organization / infrastructure, it is important that conscious sign off (on both, controls implemented, as well as dropped) is taken from senior management based on residual risk acceptable to the Organization.

- **The five families of controls are:**

  - Planning Controls for ensuring that the security is taken as a key design parameter for all new CIIs at conceptualization and design level itself.
  - Implementation Controls for translating the design/conceptualization planning into mechanisms for protecting the CII. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.
  - Operational Controls for ensuring that the desired security posture is maintained in the operational environment. These controls also come into play in case of retrofitting existing, unprotected / poorly protected CII.
  - Disaster Recovery/ Business Continuity Planning (BCP) Controls for ensuring minimum downtime and the restoration process.
  - Reporting and Accountability Controls for ensuring adequate accountability and oversight exercised by Senior management, as well as reporting to concerned Government agencies where required enforced through compliance controls.

- In circumstances where a particular control may not provide the best fit, we as an organization needs to consider compensatory controls which could also be procedural, so as to ensure that the attack surface presented by the organization's Information Infrastructure is minimized.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.