Cyber Security & Cyber Resilience Policy

. 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 stock brokers perform significant functions in providing services to holders of securities, it is desirable to have robust cyber security and cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.

. Keeping above in mind SEBI has issued circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated 03-12-2018 & have asked stock brokers to frame their policy on **Cyber Security & Cyber Resilience,** hence this policy

. The following policy shall be effective from April 1, 2019.

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 security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization’s ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

Governance

.

As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, S.A.DESHPANDE & CO.(SADCO) have formulated a comprehensive Cyber Security and Cyber

Resilience policy encompassing the framework mentioned hereunder. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, will be provided in the policy.

This policy is approved by the Partners of SADCO.The policy will be reviewed by SADCO at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.

3. The Cyber Security Policy of SADCO have included the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:
   a. 'Identify' critical IT assets and risks associated with such assets.
   b. 'Protect' assets by deploying suitable controls, tools and measures.
   c. 'Detect' incidents, anomalies and attacks through appropriate monitoring Tools/processes
   d. 'Respond 'by taking immediate steps after identification of the incident, anomaly or attack
   e. 'Recover' from incident through incident management and other appropriate Recovery mechanisms.

SADCO is not trading through APIs based terminal hence not considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of 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.

SADCO has designated **Chetan B.Shah**, partner of the firm as "Designated Officer" whose function would be 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.

SADCO shall constitute Technology Committee comprising experts. This Technology Committee shall review on a half yearly basis the implementation of the Cyber Security and Cyber Resilience policy approved by the Partners of the firm, and such review shall include review of SADCO current IT and Cyber Security and Cyber

Resilience capabilities, set goals for a target level of Cyber Resilience, and shall establish plans to improve and strengthen Cyber Security and Cyber Resilience of SADCO.

The review shall be placed before the Partners for appropriate action.

SADCO will establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.

The Designated officer and the technology committee of SADCO will periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

. SADCO will define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of SADCO towards ensuring the goal of Cyber Security.

Identification

SADCO will identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, SADCO will maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

SADCO will accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

Protection

<u>Access controls</u>

. No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities.

. Any access to SADCO systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. SADCO shall 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 shall be for the period when the access is required and shall be authorized using strong authentication mechanisms.

SADCO will implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases. Illustrative examples for this are given below

. All critical systems of SADCO accessible over the internet shall have two-factor security (such as VPNs, Firewall controls etc.)

SADCO will ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs will be maintained and stored in a secure location for a time period not less than two (2) years.

. SADCO will deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to SADCO critical systems. Such controls and measures will inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to SADCO critical systems, networks and other computer resources, shall be subject to stringent supervision, monitoring and access restrictions.

. SADCO will 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 SADCO critical IT infrastructure.

SADCO will address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

. Physical access to the critical systems shall be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors will 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 will be revoked immediately if the same is no longer required.

SADCO shall ensure that the perimeter of the critical equipment’s room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

. SADCO shall establish 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 shall be secured within SADCO premises with proper access controls.

. For algorithmic trading facilities, adequate measures shall be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.

SADCO will install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.

. Adequate controls will be deployed to address virus / malware / ransom ware attacks. These controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.

Data security

. Critical data will be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given below

Illustrative Measures for Data Security on Customer Facing Applications

1. SADCO will analyse the different kinds of sensitive data shown to the Customer on the front end application to ensure that only what is deemed absolutely necessary is transmitted and displayed.
2. Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piece of data over various networks.
3. SADCO will a nalyse data and databases holistically and draw out meaningful and "silos" (physical or virtual) into which different kinds of data can be isolated and cordoned off. For instance, a database with personal financial information need not be a part of the system or network that houses the public facing websites of the SADCO. They should ideally be in discrete silos or DMZs.
4. SADCO will implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is in feasible for certain personnel

such as System Administrators and developers to not have privileged access to databases. For such cases, SADCO will take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. SADCO will also take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.

5. SADCO will use industry standard, strong encryption algorithms (eg: RSA, AES etc.) wherever encryption is implemented. It is important to identify data that warrants encryption as encrypting all data is in feasible and may open up additional attack vectors. In addition, it is critical to identify the right personnel to be in charge of, and the right methodologies for storing the encryption keys, as any compromise to either will render the encryption useless.
6. SADCO will ensure that all critical and sensitive data is adequately backed up, and that the backup locations are adequately secured. For instance, on servers on isolated networks that have no public access endpoints, or on-premise servers or disk drives that are off-limits to unauthorized personnel. Without up-to-date backups, a meaningful recovery from a disaster or cyber-attack scenario becomes. Increasingly difficult

SADCO will implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It shall be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given below

Illustrative Measures for Data Transport Security

1. When an Application transmitting sensitive data communicates over the Internet with SADCOs' systems, it will be over a secure, encrypted channel to prevent Man- In-The-Middle (MITM) attacks, for instance, an IBT or a Back office communicating from a Customer's web browser or Desktop with SADCOs' systems over the internet, or intra or inter organizational communications. Strong transport encryption mechanisms such as TLS (Transport Layer Security, also referred to as SSL) will be used.
2. For Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured TLS (SSL) certificate on the web server

will be used making the transport channel HTTP(S).

3. SADCO will avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, will adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

. SADCO information security policy will also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.

SADCO will allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.

Hardening of Hardware and Software

SADCO will only 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 or that can be potentially used for exploitation of data will be blocked and measures will be taken to secure them.

Application Security in Customer Facing Applications

Application security for Customer facing applications offered over the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by SADCO to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative list of measures for ensuring security in such applications is provided below

Illustrative Measures for Application Authentication Security

1. Any Application offered by SADCO to Customers containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as “Application” hereafter) over the Internet shall be password protected. A reasonable minimum length (and no arbitrary maximum length cap or character class requirements) shall be enforced. While it is difficult to quantify password “complexity”, longer passphrases have more entropy and offer better security in general. SADCO shall attempt to educate Customers of these best practices.
2. Passwords, security PINs etc. will never be stored in plain text and will be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances.
3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software cryptographic tokens, VPNs, biometric devices, PK etc.).

   In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory.
4. In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.
5. After a reasonable number of failed login attempts into Applications, the Customer’s 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 Customer’s 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 SADCO that after verification of the Customer’s identity etc.
6. SADCO will avoid forcing Customers to change passwords at

frequent intervals which may result in successive, similar, and enumerated passwords. Instead, will focus on strong multi -factor authentication for security and educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication reset information (such as e-mail and phone number) are up-to-date.

7. Both successful and failed login attempts against a Customer's account may be logged for a reasonable period of time. After successive login failures, it is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins.

Certification of off-the-shelf products

SADCO will ensure that off the shelf products being used for core business functionality (such as Back office applications) shall bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardization Testing and Quality Certification (Ministry of Electronics and Information Technology). if SADCO uses Custom developed / in-house software and components than SADCO need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests shall include business logic and security controls.

Patch management

SADCO will establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation time frame for each category of patches shall be established to apply them in a timely manner.

SADCO will 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.

Disposal of data, systems and storage devices

SADCO will frame suitable policy for disposal of storage media and systems. The critical data / Information on such devices and systems will be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

SADCO will formulate a data-disposal and data- retention policy to identify the value and lifetime of various parcels of data.

Vulnerability Assessment and Penetration Testing (VAPT)

SADCO will regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.

SADCO with systems publicly available over the internet shall 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.

In addition, SADCO will perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.

. In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, SADCO will report them to the vendors and the exchanges in a timely manner.

. Remedial actions will be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

Monitoring and Detection

SADCO will establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized 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 will 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, SADCO will 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 will 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

48.The response and recovery plan of SADCO will 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. SADCO will 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

. The response plan of SADCO will define responsibilities and actions to be performed by SADCOs' employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism.

Any incident of loss or destruction of data or systems will be thoroughly analyzed and lessons learned from such incidents will be incorporated to strengthen the security mechanism and improve recovery planning and processes.

SADCO will also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.

Sharing of Information

Quarterly reports containing information on cyber-attacks and threats experienced by SADCO 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 will be submitted to Stock Exchanges / Depositories.

Training and Education

SADCO will work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).

SADCO will 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 shall be extended to outsourced staff, vendors etc.

The training programs shall be reviewed and updated 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.) of SADCO are managed by vendors and SADCO may not be able to implement some of the aforementioned guidelines directly, SADCO will 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.

Systems managed by MIIs

Where applications are offered to customers over the internet by MIIs

(Market Infrastructure Institutions), for eg.: NSE's NOW, BSE's BEST etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs and not with SADCO. SADCO is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

Periodic Audit

AS the Terms of Reference for the System Audit of Stock Brokers specified vide circular no. CIR/MRD/DMS/34/2013 dated November 06, 2013, stand modified to include audit of implementation of the aforementioned areas.

SADCO being a Type I Stock Brokers (as defined in CIR/MRD/DMS/34/2013 dated November 06, 2013) shall arrange to have their systems audited on an annual basis by a CERT-IN empanelled auditor or an independent CISA/CISM qualified auditor to check compliance with the above areas and shall submit the report to BSE LTD. Along with the comments of the Partners of SADCO within three months of the end of the financial year.

Approval by the partners of the firm

We have approved this CYBER SECURITY & CYBER RESILIENCE policy on 26-03-2019 as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the exchange/SEBI.

For S.A.DESHPANDE & CO

sd/-	**Sd/-**	**Sd/-**	**Sd/-**
(Bhupatray.L.shah)	**(Nilesh shah)**	**(paresh shah)**	**(Chetan shah)**
Partner	**Partner & Compliance** Officer	**Partner**	**Partner**