# ABIRA SECURITIES LIMITED

## CYBER SECURITY AND CYBER RESILIENCE POLICY

## 1. STATUTORY MANDATE

This framework is formed in accordance with the requirements of the SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 (“the circular”) dated December 3, 2018.

## 2. 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. Adhering to that, we are doing our bit to empower our customers by making our policies available for public viewing so that they get closer to understanding the functioning of the organization.

## 3. APPLICABILITY AND GOVERNANCE

Provisions of the said circular and framing of cyber security and cyber resilience are required to be complied with all Stockbrokers and Depository Participants registered with SEBI.
The policy has been considered, taken on record and approved by the board of directors of the company at their duly convened meeting held on 12/06/2020.

## 4. DESIGNATED OFFICER AND DUTIES OF DESIGNATED OFFICER

ASL is committed to protecting and enhance its client’s value by fulfilling their desired contractual obligations and conducting the affairs of the company in ethical and lawful manner. The Board of Directors and Senior Management are committed to adopt the Code of Conduct and its lawful policies and procedures. They shall affirm compliance by fulfilling.

their duties and responsibilities and commitment towards the company in a well desired manner.

The Company nominates **Mr. Asish Nath** as Designated Officer (DO), to assess, identify, and reduce Cyber Security risks, responds to incidents, establishes appropriate standards and controls, and directs the establishment and implementation of processes and procedures as per the Cyber Security Policy. He has the necessary freedom to act on his own authority and should report to the Board.

## 5. CONSTITUTION OF TECHNOLOGY COMMITTEE

The Board has constituted an Internal Technology Committee comprising of the following experts who are responsible for **half yearly review** of the Cyber Security and Cyber Resilience policy so approved by Board of Directors.

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

| Sr. No | Name of the Committee Members | Designation of the Members |
|---|---|---|
| **1** | **ASISH NATH** | **MANAGER IT (DO)** |
| **2** | **PALLAB CHAKRABORTY** | **COMPLIANCE OFFICER** |
| **3** | **SUDIP SAHA** | **OPERATION HEAD** |

Such committee shall on a half yearly basis review the implementation of the Cyber Security and Cyber Resilience policy. Such review shall include but not limited up to, reviewing of current IT and Cyber Security and Cyber Resilience capabilities, setting up of 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 to take appropriate action(s), if required.

## 6. PROCESS TO IDENTIFY AND PROTECT CRITICAL ASSETS

**Lists of Critical assets and its location maintained at Abira Securities Ltd (ASL)**.

- ODIN-WAVE- Application software
- MS-SQL SERVER- IBM-3650M4, X3250
- FortiGate 80E- Firewall
- CISCO ROUTER
- AVO 10 KV UPS
- Cisco Network Switch

## 7. PRINCIPLES AND PRACTICES

The company ensures compliance with the record-keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there under, PMLA Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye Laws and Circulars.

## 8. COMMUNICATION OF UNUSUAL ACTIVITIES AND EVENTS

IT team of the company under guidance of the committee shall monitor unusual activities and events and communicate the same to designated officer via **C PANEL Mail** for necessary actions, as may be required. C PANEL Mail system is used for internal and external communications.

## 9. REVIEW AND STEPS TO STRENGTHEN CYBER SECURITY FRAMEWORK

The DO and the technology committee **quarterly review** the instances and effects of cyber-attacks and thereby makes provision and steps to avoids such attacks in future by implementing various controls and tools to strengthen overall framework.

## 10. RESPONSIBILITIES OF EMPLOYEES, MEMBERS AND PARTICIPANTS

Role and responsibility of employees/staffs of ASL are as under defined:

- User accounts on company's computer systems are to be used only for business of the company and not to be used for personal activities.

- Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their login IDs and passwords.

- Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the company. Users shall not purposely engage in activity with the intent to: harass others.

- users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.

- Users shall not attach unauthorized devices on their PCs or workstations unless they have received specific authorization from the employees' manager and/or the company IT designer.

- Users shall not download unauthorized software from the Internet onto their PCs or workstations.

- Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate supervisor. They are also required to report any unusual activities and events if any noticed to the immediate supervisor and DO for the action.

- When employees are separated or disciplined, his/her limit access to systems shall be removed.

- Physically secure computer assets, so that only staff with appropriate needs can access.

- Employees who forget their password must call the IT department to get a new password assigned to their account. The employee must identify himself/herself by (e.g., employee number 00123) going to the IT department.

- Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

## 11. IDENTIFICATION

All critical assets based on their sensitivity and criticality for business operations, services and data management have been identified and marked.

Based on importance and confidentiality of the information stored in the assets, criticality of the assets is measured and so its security level is ranked accordingly.

| Security Level | Description | Example |
|---|---|---|
| RED | This system contains confidential information – information that cannot be revealed to personnel outside of the company. Even within the company, access to this information is provided on a “need to know” basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or adverse.<br>financial impact on the business of the company. | Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information. |
| GREEN | This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network. | User department PCs used to access Server and application(s). Management workstations used by systems and network administrators. |
| WHITE | This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive.<br>information or perform critical services. | A test system used by system designers and programmers to develop.<br>new computer systems. |
| BLACK | This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain.<br>confidential information. | A public Web server with non-sensitive information. |

## 12. PROTECTION

- **Access Controls**: The Company has established the following user groups and defined the access privileges and responsibilities:

| User Category | Privileges & Responsibilities |
|---|---|
| Department Users (Employees) | Access to application and databases as required for job function. (RED and/or GREEN cleared) |
| System Administrators | Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Accessto confidential information on a “need to know” basis only. |
| Security Administrator | Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function. |

| | |
|---|---|
| Systems Analyst/Programmer | Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices. |
| Contractors/Consultants | Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to company information and systems must be approved in writing by the company.<br>director/CO. |
| Other Agencies and Business Partners | Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws. |
| General Public | Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information. |

- **Password Policy:**

A Password Register is maintained which is kept with **Mr. Asish Nath** (System Head of ASL).

**Passwords used at ASL have the following characteristics:**

- All the passwords are a minimum of eight characters long.
- The passwords are a combination of alphabets and numeric.
- The password contains both upper- and lower-case characters (e.g., a-z, A-Z).
- The passwords have digits e.g., 0-9.
- The passwords are not a word in any language, slang, dialect, jargon, etc.
- The passwords have been recommended not to be based on personal information, names of family, etc.
- The password register of all the servers is verified and checked regularly by the System in-charge. All the windows login passwords, Exchange user login passwords, desktop administrator account password, default email passwords, default application passwords, system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) are kept universal at the beginning, changed on first time login, changed at every fortnightly.

- **Two-Factor Security:** All critical assets of ASL accessible over the internet have two-factor security. Firstly, it is secured and prevented with installed FortiGate 80E-Firewall at Switch node and then it is safeguarded by Anti-Virus.

- **Record maintenance**: Records of user are uniquely identified and logged for audit and review purposes. Such logs and records are maintained and stored in a **backup server** (**Software name – MS-SQL SERVER- IBM-3650M4**) for a time of **not less than 5 years**.

- **Internet access policy**: ASL runs its business on IT infrastructure. Network policy is defined in such a manner that the organization data is kept securely, safely and reliably. DP's back office is not connected to internet. Network usage is strictly allowed to the authorized users of each department. A Firewall has been implemented to prevent outside infiltrations to our network. No social media sites such as Facebook, Twitter etc. can be logged in inside the organizations by any employees.

- **Deactivation of access**: Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the company office.

## 13. PHYSICAL SECURITY

- Access to server rooms and IT equipment rooms is restricted to only those whose job responsibilities require that they maintain the equipment or infrastructure of the room.
- Access to server rooms and IT equipment rooms is controlled by a strong authentication method.
- Server rooms and IT equipment rooms is to be monitored by CCTV or IP cameras 24/7 which is under installation process.
- Server rooms and IT equipment rooms have redundant power sources, such as a generator in case of a power failure or outage.
- A complete inventory of server room and IT network room equipment, including brands, models, serial numbers, and physical descriptions are maintained and kept up to date.
- A system for securely disposing of unwanted discs, tapes, cards, hard drives, printed paper, and anything else that could contain confidential information is properly implemented.

## 14. NETWORK SECURITY MANAGEMENT

- **Device Security:** Communication and monitoring devices are typically deployed in the network for various purposes is configured properly according to requirement and accessed on the ground of given privilege and profile of users. Apart from that following measure is also taken in the context of device security as:

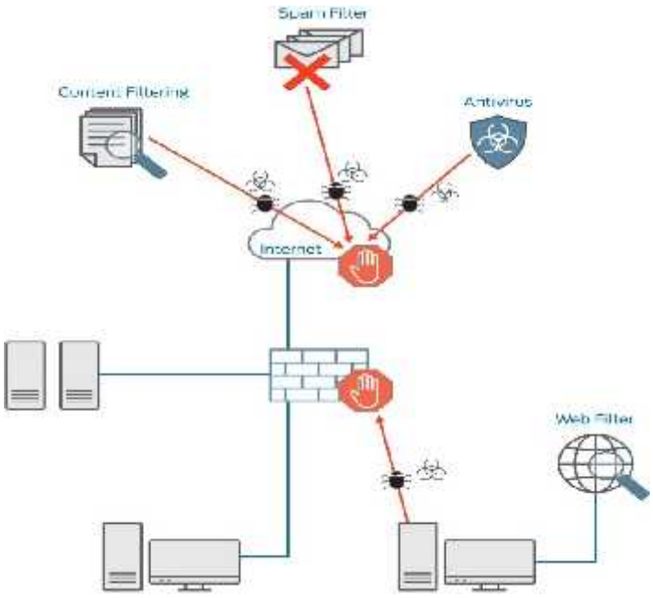
- The company has signed an NDA to system employees about not disclosing the details of deployed devices inside the perimeter as per HR policy.
- Regularly applied patches and security updates released by vendors.
- ACL is maintained to permit or deny TCP and UDP traffic.
- Services are disabled if they are not in use.

- **Firewall Rules Policy**: Firewalls are one of the most important components of the Firm's security strategy. Internet connections and other unsecured networks are separated from the company's network using a firewall. Policy rules are updated as per change in the organization's requirements such as when new applications or hosts are implemented within the network. Logs and alerts are continuously monitored to identify threats—both successful and unsuccessful. Firewall software should be patched as vendors provide updates to address vulnerabilities.

- **Intrusion detection Security:** ASL has a network intrusion detection system (NIDS) or a network intrusion protection system (NIPS) incorporated in ***FortiGate Firewall*** where it monitors inbound and outbound traffic to and from all the devices on the network. It includes inbuilt licensed Antivirus along with ***Kaspersky Endpoint Security***.

- **Virus Prevention:** IT teams are constantly faced with the challenge of protecting their companies' productivity and digital assets against evolving and sophisticated threats, including spam and phishing attacks, viruses, Trojans and spyware infected files, unapproved website access, and unapproved content. To prevent all,
- such ASL has installed inbuilt licensed Antivirus along with Kaspersky Endpoint
- Security placed between the WAN and the LAN i.e., Fortinet and internal network. It
- combines multi-layered, next-generation threat protection with additional proactive technologies such as Application, Web and Device controls, vulnerability and patch management and data encryption into an EDR-ready endpoint agent with an extensive systems management toolkit.

Here it shows how it works:




## 15. DATA SECURITY

**ASL** protects restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.
Data that must be moved within is to be transferred only via business provided secure transfer mechanisms (e.g., encrypted USB keys, file shares, email etc).

Abira takes reasonable technical and organizational precautions to prevent the loss, misuse or alteration of your personal information. Abira will store all the personal information you provide on its secure servers. Information relating to electronic transactions entered via this Website will be protected by encryption technology.

Any information being transferred on a portable device (e.g., USB stick, laptop, pen drive etc) is in line with industry best practices and applicable law and regulations.
Documents which are no longer required are shredded right away. Printer areas are kept clean by collecting the printed documents right away so that it does not reach unauthorized individuals.

## 16. HARDENING OF HARDWARE AND SOFTWARE

In **ASL**, we deploy hardened hardware/ software in order to minimize clients' risk of suffering a cyber attack, adhere to the following protocol:

- **Programs clean-up**
- **Patches and patch management**
- **Use of service packs** – Keep up-to-date and install the latest versions.
- **Group policies:** In ASL we have implemented strong passwords, secured their credentials and changed them regularly. Open ports on networks and systems which are not in use are being blocked immediately.

## 17. APPLICATION SECURITY IN CUSTOMER FACING APPLICATIONS

Today's enterprises are struggling to secure their applications. With thousands of applications in use and new threats emerging daily, large organizations face a monumental task.
So, to protect and prevent applications risks/threats, **ASL** took different security measures for applications that run on-premises depending on whether they are third-party or custom applications.

For third-party applications, the following steps been taken:

- **Remediation process:** A process for remediating or mitigating application security vulnerabilities. This should include an inventory of all applications in use at the organization, a way to track known vulnerabilities and patches, and a method for applying patches such as patch management.
- **Identity management:** ASL considers a unified identity management solution that requires the use of strong passwords.
- **Infrastructure security:** It's also worth noting that applications are only as secure as the infrastructure and networks on which they run. Security teams need to follow industry best practices such as deploying firewalls, intrusion detection and prevention systems, and other security solutions.

For security purpose, we at ASL we follow the security measures which includes that if after a reasonable number of failed login attempts into application, the customers' accounts are been set to locked state where further logins are not possible until a password and authentication reset has been performed i.e., a cryptographic secure unique link is sent to the customer account holder's registered email ID and a random OTP simultaneously sent to customer's registered mobile no. at ASL database.

## 18. CERTIFICATION OF OFF-THE SELF PRODUCTS

In **ASL**, all the software pre-built by the third-party vendors or purchased/ licensed /certified as per Exchange regulations. As we all know that if we use untested 3rd party applications then it can leave company open to the same threats as using any untested code, so the only way to ensure the safety of your third-party applications is to test them for their vulnerabilities and ensure that those vulnerabilities are remediated. Here in ASL, we have SHARE PRO which is a product of Standard Software (Vendor). It has provided live RMS concept which is unique and long way in reducing risk in the market as it captures live financial information and stock information as it is connected to back office. It helps to run operations smoothly, take care of peak load situation and handle exceptions. It has greater flexibility with Multi depository system capable of handling both CDSL & NSDL depository.

Other are ODIN Product (Developed by 63 Moons Technologies Ltd.) it offers trading in all segments at BSE, NSE, MCX, ICEX.

**SharePro** is certified by **Standard Software** used as the Back-office applications.

## 19. PATCH MANAGEMENT

Software vendors release patches to fix vulnerabilities identified after the release of a software or application. In ASL, we do manage Patch which enables patch testing and deployment which is a critical aspect of cyber security. Quick and instant responses to patch updates mitigate the chances of data breaches that can be due to unpatched software.

## 20. DISPOSAL OF DATA, SYSTEMS AND STORAGE DEVICES

The Board of Directors (the “Board”) of ASL has formulated and adopted this Archival Policy (the “Policy”) to comply with the provisions of SEBI and to ensure greater transparency.

The disclosure of material events is hosted and retained on the Company’s website for a ***minimum period of 5(five) years*** and thereafter in the archives of the Company for an additional period of 1(One) year. The contents of the Archived documents are accessible to the designated director only.

In ASL, the archival documents are not removed or destroyed or deleted from the website without the prior written approval by designated director.

All the critical data and information on devices and systems is removed by using methods such as crypto shredding or physical destruction.

## 21. VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

In ASL, VAPT has been exercised and been carried out once a year under the core guidance of experts.
Penetration tests go beyond security audits and vulnerability assessments by trying to breach the system just like a hacker. In this scenario, a security expert tries to replicate the same methods employed by bad actors to determine if IT infrastructure could withstand a similar attack. Penetration testing is a real time attack on your digital assets to reveal security weaknesses or loopholes in your infrastructure. This is the single way to find out what malicious users could access from your website or network.

Following is the step-by-step Vulnerability Assessment Methodology/ Technique


In the case of off-the-shelf products or applications, vulnerabilities or threats discovered in VAPT are reported to the vendors and the exchanges as and when occurred so that the timely solutions and remedial action can be taken.

## 22. MONITORING AND DETECTION

In ASL, necessary steps are taken to monitor and for early 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 ex ternal parties is maintained, appreciated and taken care on.

## 22. RESPONSE AND RECOVERY

The company shall consider the outcomes of any incident of loss or destruction of data or systems and accordingly shall take precautionary measures to strengthen the security mechanism and improve recovery planning and processes. Periodic checks to test the adequacy and effectiveness of the response and recover plan shall be done. 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 SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June22,2012 and subsequent revisions, if any, from time to time. In ASL, we use NAS (Network Area Storage) MS-SQL SERVER- IBM-3650M4 which is the combination of storage, computing, and networking to improve speed, especially during disaster recovery sessions. In the case of any incident response cyber attacks, we can have recovery from Back up servers.

## 23. SHARING OF INFORMATION

**Quarterly reports** containing all the information on cyber-attacks and threats experienced by ASL and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats is submitted to Stock Exchanges, as per statutory requirements / guidelines.

## 24. TRAINING AND EDUCATION

Abira Securities Limited considers all its employees as part of the family. To build strong Cyber Security and basic system hygiene awareness of staffs training sessions and workshops is a part of on-the-job training or continuing education program. These workshops are presented by experienced stockbrokers, financial advisors or financial instructors. We 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.

## 25. PERIODIC AUDIT

As per circular no. CIR/MRD/DMS/34/2013 dated November 06, 2013, System Audit shall accordingly stand modified to include audit of implementation of the aforementioned areas. As defined in CIR/MRD/DMS/34/2013 dated November 06, 2013, we arrange to have systems audited on an annual basis by a CERT-IN empanelled auditor or an independent CISA/CISM/DISA 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 ***within three months of the end of the financial year***.

## 26. UPDATES TO THIS POLICY

We update this Policy from time to time if any change takes place and will review it at least ***annually***. We encourage you to periodically check back to this Policy to learn about updates to our privacy practices.