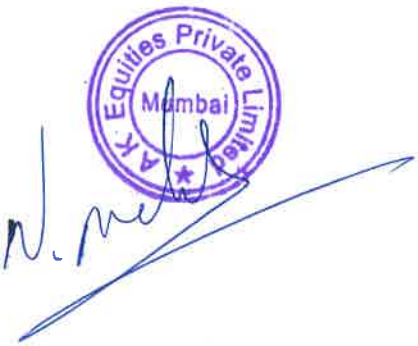
A. K. EQUITIES PVT. LTD.

SEBI REG. No. INZ000239939

Cyber Security and Cyber Resilience Policy

Version 1.0



A. K. Equities Private Limited
Registered Office: Kalpataru Heritage | 4th Floor | 127, M.G. Road | Fort | Mumbai - 400001 | T: +91 22 22703201 | +91 22 61402500
F: +91 22 61402555 | E: backoffice@akequities.com | CIN-U67190MH2000PTC124750

Distribution List

#	Name of the Custodian
1	Board of Directors:- Mr. Nimesh Mehta and Mr. Sudhir Nayak
2	Technology Committee: 1. Mr. Nimish Mehta- Director 2. Mr. Ritesh Shah- Designated Officer 3. Mr. Minissh Jadhav [Expert]
3	Designated Officer – Mr. Ritesh Shah

Glossary

- **Secure Areas** means those areas where critical devices are kept like Data Centre, Network Closets, etc.
- **Information Assets** means Applications, Web Servers, Databases, Network Devices like Router-Switches-Firewalls-IDS-IPS etc.
- **Infrastructure** means supporting devices like Physical Access Control Devices, Air Conditioners, UPS, Batteries, Power Generators, Fire Extinguishing Systems, power and data cabling, Smoke Detectors, Fire Alarms, Temperature and Humidity indicators (Hygro meter) etc.
- **"USERS"** means all users of the system including employees, third party users, contractors, temporary users, etc. unless explicitly otherwise specified.
- **Workstation –** A desktop, a laptop, a console, a smart phones or any other special device using which a USER can to the another device.
- **"Personally Identifiable Information (PII)"** means any information that relates to the Customers which either directly or indirectly, in combination with other information available or likely to be available, is capable of identifying such Customer e.g. Customer's name, age, gender, contact details, email addresses, bank details, passport number or any other information specifically classified and described accordingly in the contract, for covering with data protection controls.

Contents

Contents

AK Equities Private Limited Mumbai

1. Introduction

M/s A.K. Equities Pvt. Ltd. is registered with NSE and BSE as a Member.

M/s A.K. Equities Pvt. Ltd. trades on the Exchanges only through Exchange Terminals viz., NEAT and BOLT. It does not have CTCL Facility, does not provide IBT, Algo, STWT etc to its clients. It operates through 3 no. of terminals. It has only 1 office. It has 5 employees and has back office software of 'Comtek'. **M/s** A.K. Equities Pvt. Ltd. **comes under Type I broker category.**

This Document describes the Security Controls that should be implemented and practiced for various Information Assets, so as to ensure compliance to the Information Security Policies of **M/s. A.K. Equities Pvt. Ltd.**

The Information Security Policies are designed as per Information Security guidelines for Stock Brokers / Depository Participants by SEBI vide circulars issued on various dates mentioned above. Henceforth, these circulars listed above will be referred to as "Regulatory Guidelines" which will include SEBI, NSE, BSE, CDSL, NSDL and any other relevant regulatory body governing the business of brokers and Depository Participants.

To ensure compliance with the regulatory guidelines, a comprehensive document is prepared as under.

Structure of the document is as under

This document is divided into various sections and each section is structured as under

- **Policy Objectives :** This section broadly describes the reasons for preparing the policy.
- **Policy Scope**: This section defines various internal and external entities as well as the Information Assets to which the policy applies.
- **Policy Statement(s)**: This section describes the Information Security Policies for each control area.
- **Detailed Procedures**: This section describes the Information Security Procedures at detailed level, so as to help implement and comply with the Security Policy. However, this section does not describe the Technical details to implement these Procedures. The technical details are described in the "hardening guidelines" document.
- **Implementation Responsibilities**: This section describes the entities, who are responsible for the implementation of information security procedures for a given area.

There are certain policies and procedures in this document, the contents wherein are commonly applicable to various other policies and procedures. For e.g. password policy would be applicable to various other policies like O.S., databases, applications, etc. To avoid repetition and streamline the process of maintaining the policy, such "COMMON" policies have been defined separately and are referred where they are applicable.

2. Technology and Security Governance Policy

2.1 Policy Objective

To ensure proper direction and Governance of Information Technology and Information and Cyber Security, a committee drawn from critical functions needs to be set up.

2.2 Policy Scope

This policy covers present and proposed Information Technology set up and related activities. It also covers defining strategies and security requirements for the Information Technology and related set up and supporting activities.

2.3 Policy Statement(s)

1. Set up a Technology / Strategy / Security Committee.
2. Define roles and responsibilities of The Technology Committee
3. Define frequency for meeting of Technology Committee
4. Keep record of the Minutes of Meetings.
5. Reporting to SEBI about the status of implementation

AK Equities Private Limited Mumbai

2.4 Detailed Procedures

#	Detailed Procedures
1.	**Set up a Technology / Strategy / Security Committee**
	Organization Structure Nimish Mehta- Director Sudhir Nayak- Director Ritesh Shah- AVP-Designated Officer Avinash Bhadoria- Compliance Officer Sunil Gavas- Back Office Executive Prashant Jadhav- Office Assistant Vinay Sakpal- Office Assistant A committee of seniors and experts from various functions / departments is set up as Governance Committee. This Governance Committee will also provide direction and guidance on various matters like Technology, Strategy, Security and Cyber Resilience capabilities. Hereinafter this committee will be referred to as "Technology Committee". The Organisation structure of the "Technology Committee" is as under: **Technology Committee Members** 1. Mr. Nimish Mehta- Director 2. Mr. Ritesh Shah- Designated Officer 3. Mr. Minissh Jadhav [Expert]
2.	**Define roles and responsibilities of The Technology Committee**

The primary goal of committee is to provide Leadership and support and ensure that the Information Technology and Information and Cyber Security and Cyber Resilience requirements are aligned and integrated with the Business Security Objectives and help ensure compliance to various regulatory and legal guidelines. The Technology Committee should ensure that Information and Cyber related requirements are well Defined, documented and communicated, operationalized, monitored, reviewed and continually improved to align with the changing business and information security requirements.

Roles and Responsibilities of Technology Committee Members are as under

- **The Committee Chairperson**
  - To act as an official spokesperson in case of disaster and act as the contact person to media and newspaper.
  - To support the business through strategic direction and resolving immediate business issues and challenges.
  - To keep up with changes in business environment and map it to Information Technology Environment.
  - To provide resources for raising the level of information security awareness.
  - To approve the methodologies and processes for information security, develop road maps and strategies, prioritize the information security initiatives.
  - To ensure compliance with the legal, regulatory and contractual obligations.
  - To maintain a repository of all the critical passwords handed over by the information asset owners in sealed envelopes.
- **The Alternate Committee Chairperson**
  - Take over as Chair Person in the absence of the normal Committee Chair Person.
  - Perform all the functions listed for the Committee Chairperson above.
- **IT Head**
  - To implement the decisions taken by Technology Committee.

AK Equities Private Limited Mumbai

	○ To define roles and responsibilities for various IT Department users / teams. ○ To keep contact with authorities, support vendors etc. ○ To keep contact with special interest groups. ○ Monitor and manage security incidents. ○ To manage to People, Process, Technology. ○ Monitoring and management of systems, administrators, IT operations, Users, Authentication and Authorisation, Anti Virus set up, backup, log / audit trail etc.. ○ To ensure that security requirements are met while acquiring or developing a new system. ○ To ensure correct processing of the information. ○ To handle licensing issues. ○ To develop, implement and test Business Continuity Plan and Disaster Recovery Plan (BCP and DRP). ○ **Designated Officer** ○ To act as the executive owner of the Information Security and Cyber Security and Cyber Resilience Policies. ○ To identify the security requirements of the organization. ○ To manage Security Architecture. ○ To formulate and review information security and Cyber Security and Cyber Resilience policies and procedures. ○ To keep contact with authorities and special Interest Groups like the Cyber Police, Cyber lawyer. ISACA member group, CISO groups, Security Groups, attending security related events etc. ○ To perform and review Risks Assessment for Assets. ○ To take measures to mitigate the risk to the business information and Information processing facilities and ensure that the risks are within acceptable levels. If the risks cannot be mitigated, obtain approval for such non-implementations / Exceptions. ○ To record and maintain the Minutes of Technology Committee Meetings.

AK Equities Private Limited Mumbai

- To quarterly review instances of Cyber attack, if any domestically and globally and steps taken to strengthen cyber security and cyber resilience framework.

- **Legal & Compliance**
  - To identify the legal, regulatory and contractual obligations and ensure compliance with them.
  - To establish a procedure of obtaining Non-Disclosure Agreements from USERs.
  - Ensure timely reporting to the Regulatory Bodies like NSE, BSE, SEBI etc.
- **General Administration**
  - To ensure the physical and environmental security controls over Secure Areas (Data Centre, Air Conditioning Units, Fire Extinguishers etc. are implemented, reviewed and monitored..
  - Maintain contact details of support functions such as courier, Physical Security Guards, Access Control Device vendor, Air Conditioning, UPS, CCTV, Extinguishers etc. are available during disasters.
  - Maintain contact details for hospitals, police, fire station etc.
- **Human Resources**
  - To ensure that security controls are practiced at the three stages of employment of any USER – Before Employment, During Employment and After Employment
  - To ensure that information security responsibilities are intimated from the stage of induction.
  - To ensure that thorough background checks are carried out for potential employees of JM Financial before commencement of employment.
  - To establish a procedure of obtaining Non-Disclosure Agreements from employees.
  - To impart Security & Process training and job profile awareness training.

JM Financial Equities Private Limited Mumbai

	○ To ensure proper segregation of duties. To ensure that during EXIT process, any devices, material, etc. given to the USER are returned back e.g. a Laptop, a mobile, User ID, Access Card etc.
3.	**Define frequency for meeting of Technology Committee**
	The Technology Committee should meet at least once every half year. However, the Technology Committee should meet more often as required in case of an incident, disaster, major change of IT set up etc. The Committee should review their current IT and Cyber Security and Cyber Resilience capabilities, set goals for a target level of Cyber Resilience, and establish plans to improve and strengthen Cyber Security and Cyber Resilience. The review shall be placed before the Board / Partners / Proprietor of the Stock Brokers / Depository Participants for appropriate action. (SEBI Circular dated 3rd Dec 2018)
4.	**Keep record of the Minutes of Meetings.**
	The Designated Officer should record and safe keep the Minutes of Meetings. In the Minutes, he should record details such as the agenda, keep attendance details, date, time and duration of meeting, business transacted, Any business if unfinished, decisions taken on various items etc.
5.	**Reporting to SEBI about the status of implementation**
	The Designated Officer should communicate to SEBI, the status of implementation of the provisions of the circular dated 3rd Dec 2018, in their monthly report

2.5 Implementation Responsibilities

- Members of the Technology Committee are jointly responsible for implementation of the policies.

3. Asset Management Policy

3.1 Policy Objective

The purpose of this policy is to define the parameters for proper management of assets. These guidelines are defined to ensure streamlining of asset procurement, maintenance and disposal. Inappropriate procurement / installation exposes to various risks including virus attacks, compromise of network systems and services, and legal issues.

3.2 Policy Scope

This policy covers all information assets supporting the business activities and is applicable to all USERS.

3.3 Policy Statements

1. Controls over procurement of IT Assets and Services.
2. Maintain up-to-date information asset inventory register.
3. Information assets should be tagged / labelled appropriately.
4. Optimal utilization of IT Assets and Services should be ensured.
5. Assets should be properly maintained.
6. Assets should be adequately insured.
7. Security of Information Assets during operations
8. Controls over Movement of Assets.
9. Controls over retirement of Information Assets.
10. Controls over disposal of information assets.

3.4 Detailed Procedures

#	Detailed Procedures
1.	**Controls over procurement of IT Assets and Services.**
	All information assets should be procured after receiving proper requisition in writing from the respective department heads. The requisitions received, should be discussed in the next Technology / IS Committee meeting and if found to be in order, procurement process should be initiated. If required, the Technology / IS committee may decide to seek further details / clarifications from the concerned department head. Where necessary, multiple quotations would be sought and comparison / negotiations would be carried out before placing the order for procurement.
2.	**Maintain up-to-date information asset inventory register.**
	An up-to-date information asset inventory should be maintained by the respective asset custodians. It should be the responsibility of all the department heads to provide the necessary information about the information assets within their departments as and when asked for. Information such as Asset Owner, Asset Custodian, Location of the asset, Risk Owner, CIA (Confidentiality, Integrity, Availability) details etc. should be entered into the Asset Register.
3.	**Information assets should be tagged / labelled appropriately.**
	Where required, the information assets should be labelled with the asset code stickers for easy identification. A asset naming convention should be defined and consistently followed for labelling.
4.	**Optimal utilization of IT Assets and Services should be ensured**
	• Information assets should be used only for official purpose. • In case any user notices that an information asset is being under-utilised or is under-performing, he / she should inform the CISO / CTO who should initiate appropriate actions.

	• Any changes / modifications to settings / configuration of information assets should be carried out by authorised and qualified personnel only.
5.	**Assets should be properly maintained.**
	• All the information assets should be maintained as per recommendations of the respective Original Equipment Manufacturer (OEM). • Appropriate records for maintenance of information assets should be kept.
6.	**Assets should be adequately insured**
	Asset owners / Departmental Heads / General Administration should ensure that the IT Assets are adequately insured against the relevant threats. A record of such insurance policies should be maintained.
7.	**Security of Information Assets during operations**
	Though asset owners are primarily responsible for security of their respective information assets, it is also the responsibility of all USERS to ensure that the information assets being handled by them are safeguarded against damage, misuse, theft, etc. Further, no information asset should be removed from the premises without appropriate authorisation.
8.	**Controls over Movement of Assets**
	• When any information asset is in transit, then the personnel carrying the same should be responsible for its security. • Reliable transport or courier agency should be used. A list of authorized couriers should be agreed and the procedure to check the identification for the couriers should be implemented. • Packaging should be adequate to protect the contents from any physical damage. • Record of all in-transit information assets should be maintained.
9.	**Controls over Retirement of Information Assets**

	• Each information asset has a functional life and needs replacement at the end of its functional life. "End of Support" (EOS) dates for IT Systems and Software should be closely monitored to ensure that information assets are not exposed to security risks due to unavailability of security patches / spares from the Original Equipment Manufacturer (OEM). • Generally, the information assets should be replaced, when they become a hindrance in the performance of day-to-day activities. • Whenever a user faces performance issues with the information asset, he / she should inform the IT Department who will perform the necessary diagnostics on the information asset. • If the information asset is deemed to be "Beyond Repair", the IT Department should inform the concerned Head of Department as well as the procurement team that the information asset needs to be replaced. • Once the information asset is replaced, the IT Department should remove the old information asset and start the disposal process.
10.	**Controls over Disposal of Information Assets**
	• All the information assets should be disposed securely and safely when no longer required. • In case of records like paper documents, the same should be destroyed using a paper shredder after the prescribed period of time • In case of disposal of IT equipment, the information / data should be irreversibly deleted before the equipment is disposed off.

3.5 Implementation Responsibilities

- Information Asset Owners
- Information Asset Custodians
- IT Support Team
- Department Heads
- All USERS


Equities Private Limited
Mumbai

4. Asset Classification and Risk Management Policy

• Asset Classification Scheme

Considering the business requirements, the Organisation has decided to classify its' Business Information into 3 types – Public, Internal and Confidential. The value for **"Confidentiality"** as mentioned in the Asset Inventory will be used as the basis of Classification. The Confidentiality value is decided by the Asset Owner.

Relation between the "Confidentiality" value and classification of an asset is explained below. For Classification purpose "an Asset" includes soft as well as hard copy assets.

CLASSIFICATON TYPES ARE AS UNDER

1. **PUBLIC:**

   Any asset which has a "CONFIDENTIALITY" value as "1", will be classified as PUBLIC. No other values of confidentiality (1 and 2) can be classified as "PUBLIC". This classification includes any information that may be distributed to outside of the organisation without causing any damage to the organization, its employees and stakeholders. The Management should approve any information as PUBLIC before it can be treated accordingly. E.g. Marketing materials authorized for public release such as advertisements, brochures, Internet Web pages, etc.

2. **INTERNAL :**

   Any asset which has a "CONFIDENTIALITY" value as 2 will be classified as "INTERNAL". This includes information whose unauthorized disclosure, particularly outside of the organization, would be inappropriate. The Management should approve any information as INTERNAL before it can be treated accordingly. Each such information needs approval of the management before it can be shared outside of the organisation. Most of the corporate information falls into this category. e.g. Internal memos, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories,. transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, intranet Web pages.

3. **CONFIDENTIAL :**

   Any asset which has a "CONFIDENTIALITY" value as "3", will be classified as CONFIDENTIAL. Other values (1 and 2) cannot be classified as "CONFIDENTIAL". Highly sensitive or valuable information, both proprietary and personal will fall under this category. The Management should approve such information as CONFIDENTIAL before it can be treated accordingly. Such information must not be disclosed outside of the

AK Equities Private Limited Mumbai

organization without the explicit permission of the asset owner / authorized user. E.g. Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal information (such as employee HR records, Social Security Numbers), most accounting data, merger/acquisition plans, new product launches, and other highly sensitive or valuable proprietary information

5. Risk Management Policy

In any business, Risk Management plays an important role. Almost every business decision requires executives and managers to balance risk and reward. Effectively managing the business risks is essential to an enterprise's success.

Risk Assessment exercise will be performed by determining the asset criticality based on CIA (Confidentiality, Integrity, Availability) values of the asset, by assessing risks against which protection is required and by applying standards and implementing procedures to reduce these risks to an extent, that is commercially and operationally acceptable to The Organisation.

This involves:

- Preparation of Inventory of various Information Assets under various Asset Types
- Deciding the values for Confidentiality, Integrity and Availability for each Information Asset.
- Based on these values of CIA, deciding the level of criticality of the asset.
- Identifying threats to each information asset
- Identifying status of implementation controls to mitigate each threat for each information asset
- Deciding the vulnerability based on the status of implementation of each control for each information asset
- Calculating the 'Initial Risk Factor' for each control for each asset
- If the "Initial Risk factor" for any control is less than 18, then the "Initial Risk factor" will be accepted as business risk and no further treatment or exception will be required. However, if the "Initial Risk Factor" is equal to more than 18, the control must be implemented or an Exception should be obtained.

5.1 Steps for Risk Management

#	Objective	Risk Management Activities
1.	Define Scope	Identify the Scope for Risk Assessment
2.	Preparation of Asset Inventory	Preparing the Asset Inventory with following details: • Asset Name/Hostname • Asset Type • Asset Description • Asset Custodian • Asset / Risk Owner

		• CIA Values
3.	**C-I-A Values** Defining the Criticality of the Asset	The CIA Values shall determine criticality of the asset. a) Confidentiality - Ensuring that access to information is appropriately authorized. b) Integrity - Safeguarding the accuracy and completeness of information and processing methods c) Availability - Ensuring that authorized users have access to information whenever required. These values can be 1, 2 or 3. Asset criticality shall be defined as: • Asset will be classified as Non-Critical (1) if all three CIA values are "1". • Asset will be classified as Moderately Critical (2) if any of the CIA value is "2". • Asset will be classified as Critical (3) if any one of the CIA value is "3".
4.	**THREAT Value** Identifying the threats & their impact	Based on the Asset Type, appropriate threats shall be identified. These threats shall carry a value of 1, 2 and 3 depending on the impact of threat.
5.	**INITIAL IMPLEMENTATION Value** Implementing controls to mitigate the threats	This status of control implementation will carry a value as follows: • If a control is already implemented, the value will be "1". • If a control is not implemented, the value will be "2".
5.	**VULNERABILITY Value** Identifying the Vulnerabilities	If a control is not implemented to mitigate a threat, it results in a vulnerability. This vulnerability shall be evaluated as follows: • If a control is implemented, the value of vulnerability will be 1. • If a control is not implemented, the value of vulnerability will be 3.
6.	**INITIAL RISK VALUE** Calculating the Initial Risk Factor and defining the	For calculating the **"Initial Risk factor"** for each control, the values of Asset Criticality, Threat Impact, status of Control Implementation and Vulnerability will be multiplied.

	threshold for acceptable risk.	The Organization has accepted that any risk factor which is *equal to 18 or higher* deserves Implementation of Risk Treatment Plan. Any value which is less than 18 is accepted as "Business Risk"
7.	**RTP or EXCEPTION** Defining the Risk Treatment Plan & Exception Criteria	The Organisation has decided to adopt the Risk Treatment Plan as under: 1) Implement the control and reduce the Risk Factor below 18 OR 2) Take an exception and document it as an "Accepted Risk" Exception should be taken for all instances where the Risk Factor is *equal to 18 or higher.* Appropriate reasons and with approval details shall be documented.
8.	**REVISED RISK VALUE** Arriving at Revised Implementation and Vulnerability values" and Final Risk Value.	If appropriate reasons and approvals are documented and mentioned, the Vulnerability shall be reduced to "2" since the business is aware of the risk. Final Risk Factor should be calculated by taking the revised vulnerability into consideration.

This Risk Factor Calculation addresses Risk Management in following ways:

- If the asset is **Critical**, **every non-implementation of control** irrespective of Threat Value shall be subjected to implementation of RTP or taking approval for non-implementation of RTP.
- If the asset is **Moderately Critical**, non-implementation of controls for **threats with "High" and "Moderate" impact** shall be subjected to implementation of RTP.
- If the asset is **Non-Critical**, non-implementation of controls for **threats with only "High"** impact shall be subjected to implementation of RTP.

A.K. Equities Private Limited Mumbai

6. Acceptable Usage Policy

6.1 Policy Objective

Objective of this policy is to outline the acceptable use of computer equipment and information assets.

6.2 Policy Scope

This policy covers all information assets supporting the business activities and is applicable to all USERS.

6.3 Policy Statements

1. Information assets to be used for official purpose.
2. Every USER should adhere to the Policies and Procedures.
3. Prudent limited personal usage is permitted.
4. Information Assets should be monitored for policy compliance.
5. Installations and configurations by Authorised USERS only.
6. Users to take reasonable measures to protect the equipment.

6.4 Detailed Procedures

#	Detailed Procedures
1.	**Information assets to be used for official purpose.**
	USERS must use the Information / Data and Information Processing Assets, for business purposes and in serving the interest of The Organisation, its clients and customers in the course of normal operations.
2.	**Every USER should adhere to the Policies and Procedures.**
	Effective security is a team effort involving the participation and support of every USER, who deals with information and information systems. It is the responsibility of every USER to read and understand the Information Security Procedures, and to conduct their activities accordingly.
3.	**Prudent limited personal usage is permitted.**
	Users are given access to various information assets like Computer Desktops/Laptops, e-mail facility, Internet Facility, USB Drives, etc. to help perform the day to day operations.

	Although these Information Assets are expected to be used for Business Purposes only, the Management understands and permits USERS to use these Information Assets for a "limited personal usage" e.g. the users may store reasonable amount of personal data on the organization's assets as far as it does not produce hindrance to the functionality OR is not conflicting with the organization's policies, OR USERS may be allowed limited access to the internet to view their personal e-mails etc. Final judgement about whether the "personal usage" was "limited" or not would be with the management. While the Management desires to provide a reasonable level of privacy, users should be aware that any personal data that they create / copy on the corporate systems can be tracked and monitored as and when required.
4.	**Information Assets should be monitored for policy compliance.**
	USERS should understand that the Information Assets are subject to being monitored including the personal data, emails and internet logs.
5.	**Installations and Configurations by Authorised USERS only**
	Only authorised users from IT department should carry out the installations and changes to configurations. Other USERS should not add or remove the hardware or applications.
6.	**Users to take reasonable measures to protect the equipment**
	Users should take reasonable precautions and measures to secure the equipment provided to them as they would take for their own assets.

6.5 Implementation Responsibilities

- IT Support Team
- All USERS

7. Application Security Policy

7.1 Policy Objective

- Interfaces are an extension of the Applications and hence for the purpose of this policy, Applications will also include associated interfaces which are required to complete the business function.
- Application should meet the business and user requirements.
- Application should comply with various security requirements like authentication, authorisation and auditing controls.
- Adequate controls are built into the Application software to prevent loss, modification or misuse of data.
- Changes to the Application systems are controlled and are done as per the change management policy.
- Application should generate adequate and secure audit trails to help establish accountability.

7.2 Policy Scope

This policy is applicable to all Applications installed and used within the environment and is applicable to all USERs.

7.3 Policy Statements

1. The administration of each Application should be identified and the roles and responsibilities should be defined, documented and communicated.
2. Up-to-date Inventory of the Applications should be maintained.
3. Application owners should ensure safe custody of installation kits for applications owned by them.
4. Only those components in applications which are necessary for the business should be installed.
5. Procedures should be established for ensuring integrity of the systems.
6. Appropriate Input, Process and Output controls should be defined, designed, developed, implemented and tested.
7. Controls over interfaces and intermediate Files should be established.
8. Each application should be tested for business functionality and security before being moved into production environment.
9. Scripts which are developed outside of the Application for additional functionality should be tested, documented and integrity control maintained.
10. Procedures should be established for securing critical systems.

A.K. Equities Private Limited Mumbai

11. Procedures should be established for certification of core business functionalities.

7.4 Detailed Procedures

#	Detailed Procedures
1.	**The Administrator – Roles and Responsibilities**
	The administration of the Application should be identified and the roles and responsibilities should be defined, documented and communicated. The administrator should be given adequate training on the roles and responsibilities.
2.	**Asset Inventory to be maintained**
	The Application Administrator should maintain an up-to-date Inventory of the Applications and associated interfaces, giving details as are necessary including location (PATH), name of the vendor, name of the application custodian, business supported, history of upgrades, details of Annual Maintenance Contract etc.
3.	**Controls over Installation kit**
	The Application administrator should ensure that the Application setup files and Installation KIT is are stored securely. This will help ensure that the application is not installed on unwanted systems and help ensure against unlicensed installations of the Application System.
4.	**Only the required components to be Installed**
	Only those components which are necessary for the business should be installed. This will help ensure that the system is not supporting unnecessary services and associated vulnerabilities are eliminated.
5.	**Controls over Integrity of the System**
	A systemic control should be implemented to check integrity of the core system. E.g. the administrator / Application Service Provider should consider implementing the hash / check sum controls to check the Integrity of the systems at regular intervals.
6.	**Input, Processing and Output Controls**
	Various types of "Input, Processing and Output Controls" should be defined, designed, developed, implemented and tested during the User Acceptance Testing as under
	Input Controls
	Various Input controls like Authentication Checks, Authorisation Checks, Edit Checks, Range Checks, Duplicate Checks, Existence Checks, Field Checks and Batch Controls etc. should be defined by the business users and designed and implemented by the Application Vendor / development team.

	Appropriate security measures should be built to ensure that the users cannot override/by-pass the input controls and push invalid data e.g. validation of the input should be done at the server side rather than the client side.
	Processing Controls
	During processing of various inputs, the Application should be designed to exercise adequate controls. E.g. 1. The password should not be visible and should not be susceptible to capture to any user including the Administrator in any manner including from processes and memory dumps of the Operating System. 2. Errors should be handled appropriately 3. Logs for financial and non-financial transactions should be generated and stored securely for all activities done by ALL Users including even the Administrator and privileged user IDs.
	Output Controls
	• On the client terminals, only the extremely essential sensitive data should be displayed. • Wherever possible MASK portions of sensitive data. For instance, instead of displaying the full bank account number, display only a portion of it, which is enough for the Customer to identify, but useless to an unscrupulous party who may want to covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something similar 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. • The outputs could be printouts or intermediate data files to be used in the next chain of processes in which case appropriate checks should be implemented to ensure integrity of these intermediate files. • Appropriate controls should be implemented to ensure that these outputs are not abused OR cannot be accessed by unauthorized users
7.	**Controls over Interfaces and Intermediate Files**
	The Interfaces / upload facilities / intermediate files used in the Application should be controlled for type of file, size of file, integrity checking, confidentiality of the contents and secured against unauthorized modification and copying. The interface scripts should not embed database connection stringsand should be access controlled against unauthorised modifications. The interface scripts should have an inbuilt mechanism of checking integrity at the time of each execution, to ensure against unauthorised changes.

AK Equities Private Limited Mumbai

	The application programming interfaces (APIs) should follow the guidelines as mentioned in the government regulatory guidelines and international standards like ISO 27001, COBIT, and NCIIPC etc. wherever applicable.
8.	**User Acceptance Testing**
	The Application should be tested for business functionality and security before it is moved into production environment.
9.	**Controls over scripts developed outside of the Application**
	Any scripts which are developed outside of the Application for additional functionality should be tested, documented and integrity control maintained. Further access these scripts should be controlled on the Operating Systems and / databases.
10.	**Controls for securing critical systems**
	• Wherever applicable, adequate measures should be taken to isolate and secure the perimeter and connectivity of critical systems such as E-Mail servers, application/database servers, trading systems etc. • Critical data should be identified and isolated into different physical or virtual "silos" and such silos should be accessed during processing or displayed only when explicitly requested by the customer. 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 Stock Broker. They should ideally be in discrete silos or DMZs. • Identify data that warrants encryption. Such data should be encrypted using strong algorithms like RSA, AEC etc. Further the "KEYs" used for encrypting such data should be kept under the custody of identified USERs only.
11.	**Certification of off-the-shelf products**
	Where "off-the-shelf" products are used for core business functionality (such as back office applications), such applications should bear Indian Common criteria certification of Evaluation Assurance Level 4. Custom developed / in-house software and components need not obtain the above certification, but have to undergo intensive regression testing, configuration testing etc. which should include business logic as well as security controls.

7.5 Implementation Responsibilities

- Department Heads
- Application Administrator/s and Application Service Provider/s
- The Application Maintenance Team

AK Equities Private Limited Mumbai

8. Database Security Policy

8.1 Policy Objective

- To define appropriate controls to ensure that databases are adequately secured, logged and monitored.
- Database systems are kept with latest patches and upgrades
- Appropriate backup strategy is defined to ensure business continuity.

8.2 Policy Scope

This policy is applicable to all databases and is applicable to all USERs.

8.3 Policy Statement(s)

1. Ownership should be established for each database.
2. Procedures should be established for installation and upgrade of databases.
3. Access to database should be controlled.
4. Databases should be monitored regularly.
5. Transaction logs should be monitored regularly.
6. Critical databases should be mirrored on separate disks.
7. Procedures should be established for backup / recovery of databases.
8. Procedures should be established for security of databases.
9. Procedures should be established for controls over scheduled jobs
10. Procedures should be established for segregation of development-test and production environments
11. Procedures should be established to ensure that passwords are not stored in script/configuration files
12. Procedures should be established to ensure that stored procedures, functions and triggers are encrypted
13. Procedures should be established for passwords pertaining to application systems

8.4 Detailed Procedures

#	Detailed Procedures
1.	**Database Ownership**
	• The Application Owner should be responsible for confidentiality, integrity and availability of the Database. • The Application Owner should ensure that the Operating System on which the Database has been installed is appropriately secured.

2.	**Procedures for Database installation and Upgrade**
	• Identify, document and test the security features of the Database before installation to the production sites. • Monitor the latest upgrades available for any Database and released by the DB vendor. These upgrades should be tested to evaluate the impact before installation in the production database. • Define and implement the security controls for the Database • As a best practice the database should be installed in a separate drive / folder, segregating it from the application program files.
3.	**Control over access to Database**
	• OS level file and directory permissions should be restricted and the access should be given "On Need" basis. • Access to database records and related files for users should be restricted through application only. • Immediately after installation, the passwords for default DB users should be changed before migrating into production environment. Password change for default DB users should be enforced / procedurally followed. • Users should be created on the DB only "On Need" basis, with restricted permissions, and granting of privileged rights should be avoided. • System and Database Administrator roles should be segregated. Ensure that the built-in-administrator is not a member of the "sysadmin" roles. • Command prompt on the SQL server should be disabled, if not required
4.	**Databases must be monitored regularly**
	Free space in the databases should be regularly monitored and new space be added after considering the requirements in consultation with the database/application owner/s.
5.	**Transaction logs monitoring**
	Transaction logs disk space should be continuously monitored.
6.	**Critical database mirroring**
	Critical databases should be mirrored on separate disks for recovery from system, file, or component failure.
7.	**Backup / Recovery procedures**
	Properly documented backup / recovery procedures should be in place. This documentation should contain information about type of backup, periodicity, location, restoration, testing and other relevant details.
8.	**Security of database**
	• To ensure integrity of the production database, it should be segregated from the test and development database.

A.K. Equities Private Limited Mumbai

	• To ensure confidentiality, production data should NOT be populated into the development/test environment unless authorized. The production data should be thoroughly "sanitized" before it is populated in the Test and / or development environment. • Access to data stored on tape backups, data mirrors or any derived exported data should be restricted by using appropriate security controls. • Detailed hardening document should be prepared for each type of database platform. All databases created for / being moved to production environment should be subjected to the hardening process as specified in this document. • If feasible, default port numbers for databases should be changed.
9.	**Controls over scheduled jobs**
	• Job Scheduling should be granted to only selected users. • Scheduled jobs should be periodically monitored.
10.	**Segregation development-test and production environments**
	• Production environment should be kept separate from the test and development environment. • The production environment should not be populated into test or development environment without adequate sanitization.
11.	**Password not be stored in script/configuration files**
	• Passwords should not be stored in any configuration files / scripts. If there is a need to store them, then the configuration files / scripts must be encrypted. • Field level data like passwords should be encrypted, taking into consideration the business, technical, regulatory and contractual requirements.
12.	**Stored procedures, functions and triggers to be encrypted**
	Stored procedures, functions and triggers should be encrypted on the production environment.
13.	**Password for Application Systems**
	• Passwords for Application Systems should be stored in the database in an encrypted form only. • Wherever possible, the Application User ID should be integrated with the Active Directory.

8.5 Implementation Responsibilities

- Manager – IT Service
- Chief Technology Officer

9. Network Security Policy

9.1 Policy Objective

- Only those services which are required for the business operations are enabled.
- Ensure integrity and availability of the network infrastructure.
- Ensure that the external connections (inward and outward) are controlled as per business requirements
- Private/trusted network is adequately protected against the threats from public/un-trusted network

9.2 Policy Scope -

This policy is applicable to the LAN, WAN and all Network Devices like Switches, Routers, Firewalls etc. including Remote access to and from the network and is applicable to all USERs.

9.3 Policy Statement(s)

1. Ownership of network assets should be established
2. Up-to-date network diagrams should be maintained
3. Procedures should be established to ensure that all the network equipment are tested before moving into production environment
4. IPs should be based on network design
5. Procedures should be established for segregation in network
6. Adequate redundancy should be built into the network design
7. Default passwords of all network equipment should be changed immediately after installation
8. Procedures should be established for identification of network components
9. Procedures should be established for network routing control
10. Procedures should be established for packet filtering / blocking rules
11. Unused Interfaces, services and ports should be disabled
12. Procedures should be established for use of Firewalls, Intrusion Detection and Prevention System
13. Procedures should be established for network monitoring
14. Procedures should be established for network browsing
15. Procedures should be established for access authentication
16. Procedures should be established for safekeeping of network sniffers

AK Equities Private Limited Mumbai

17. Procedures should be established for third party access to network
18. Procedures should be established for remote access security
19. Procedures should be established for remote diagnostic and configuration port protection
20. Procedures should be established for network connection control.

9.4 Detailed Procedures

#	Detailed Procedures
1.	**Assigning Ownership**
	Since Networking Assets are shared across all the departments and users, "The Chief Technology Officer" will be the Owner of the Network Assets.
2.	**Network Diagram**
	• The IT Head will be primarily responsible for defining the Network Design and maintaining an updated diagram. • Periodic reviews must be conducted to ensure that the diagram is updated to reflect the current network architecture.
3.	**Adequate Testing**
	Each Network Component should be adequately tested before moving into production environment. The test report should be held on record.
4.	**Assigning IP to network equipment**
	IP assignment to network equipment should be based on the network design.
5.	**Segregation in networks**
	• Based on the Business needs, the networks should be suitably segregated into LAN, WAN and De-Militarized Zone to help manage, secure and monitor the segments. • Various types of assets should be identified in different zones / domains and controlled through appropriate IP Addressing schemes.
6.	**Redundancy of Network Components**
	To ensure business continuity (availability of Network), adequate redundancy should be built into the Network Design.
7.	**Default Passwords to be changed**
	Default passwords of all network equipment (e.g. routers, switches) must be changed immediately after installation. Blank passwords should not be accepted by the system. Similarly the default community strings must be changed to something which is not guessable.

8.	**Network components**
	• Network administrators must ensure that all network components (e.g., terminals, communication nodes, controllers, remote processors, etc.) are uniquely identifiable and labelled using a unique coding system. The use of network components must be restricted for the intended business functions only. • Hardwired communication lines (e.g., network lines, telephone lines, etc.) must be catalogued and be uniquely identifiable to the system being accessed to facilitate discovery of wiretaps.
9.	**Network routing control**
	• Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the confidentiality of data. • Routing controls should be based on positive source and destination address checking mechanisms.
10.	**Packet filtering / blocking rules:**
	Following rules should be considered for adequate protection of network and the data: • On the interface connected to the external / untrusted networks, block packets coming from outside (untrusted) networks that are obviously fake or have source or destination addresses that are reversed. • Similarly on the interfaces connected to the external / untrusted networks, block incoming packets that claim to have source IP of any internal (trusted) network. • Drop incoming packets with loop back addresses (127.0.0.0) • If the network does not need IP multicast, then block multicast packets • Block broadcast packets (Note: this may block the DHCP and BOOTP services, but these services should not be used on the external interfaces and certainly should no cross border routers) • Block ICMP echo, redirect and mask request messages from outside as these are frequently used by attackers. . • Block incoming packets that claim to have same destination and source IP. • SNMP should be disabled or enabled with good community strings and Access Control Lists (ACLs).
11.	**Unused Interfaces, services and ports to be disabled**
	• All unused Interfaces and VTYs should be disabled or shutdown. • All unnecessary services and ports must be commented out / closed in the configuration files to prevent unauthorized use of these services.
12.	**Use of Firewalls, Intrusion Detection and Prevention System**
	• Any third party (outside) connection to or from corporate Network (LAN / WAN) must pass through a Firewall.

	• Even the critical systems on the LAN / WAN should be controlled with a network and host based firewall. • Secure communication protocols for transmissions between access points and wireless clients, should be implemented while deploying WLAN (Wireless Local Area Network), to secure the corporate network from unauthorised access. • Use of Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS): - Any third party (outside) connection to or from Corporate Network (LAN / WAN) must pass through a Firewall and should be monitored using IDS and IPS. • Even the critical systems on the LAN / WAN should be similarly controlled with an IDS and IPS. • Usage of next-generation firewalls should be ensured in case separate IDS and IPS systems are not deployed.
13.	**Network monitoring**
	• A suitable Network Management System (NMS) should be implemented. • Monitoring / detection activities which are an integral part of network management must be performed on a real-time basis • Regular enforcement checks based on the criticality of network assets should be conducted to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation.
14.	**Network browsing**
	• Users must not access areas on the network for which they do not have permission. • Network Administrators, where feasible, should use access control lists on routers to restrict unauthorized users from accessing the routers. • All hosts that run applications or contain data that are non-public should be isolated behind a firewall from external networks or appropriate access controls should be placed. • All traffic from inside the company to external networks, and vice-versa, must pass through the firewall. Only authorized traffic, as defined by the Network Administrator, must be allowed to pass.
15.	**Access authentication**
	The host operating system must validate each user prior to allowing network access. Once verified, users must automatically be directed to applications for which they have been authorized.
16.	**Network sniffers**
	Safekeeping of network sniffers (LAN/WAN) should be the responsibility of the Chief Information Security Officer. Administrators should use network sniffers during troubleshooting with the approval of the Chief Information Security Officer. All network components including desktops, laptops, servers, routers, switches, firewalls etc. should undergo hardening process as per the policy.

A-K Equities Private Limited Mumbai

17.	**Third Party access to network**
	• Before allowing third party connectivity to the corporate network, the Network Administrator must obtain the approval from Chief Technology Officer as well as the respective Group Head. • Temporary User ID and password must be granted with minimum rights that are required to perform the job. • Logs of activities (e.g., resources accessed, system or application start-stop with user identity and time of action) carried out by maintenance personnel must be generated and closely monitored by the Network Administrator.
18.	**Remote Access Security**
	• Authentication of remote users should be done using two factor authentications like hardware tokens, or a challenge/response etc. • Where necessary, Dial-back procedures and controls should be used, e.g. using dial-back modems which can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. • Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a shared computer facility. Cryptographic techniques, e.g. based on machine certificates, can be used for node authentication. This is part of several VPN based solutions. • A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application and hence users must not use 'save credentials' or 'auto logon' features.
19.	**Remote diagnostic and configuration port protection**
	Appropriate physical and logical controls should be placed over the diagnostic and configuration ports as non-protection can lead to unauthorised access.
20.	**Network connection control**
	The capability of users to connect to the network should be restricted, in line with the established policies and requirements of the business applications
21.	**Secure Data Transmission over Network**
	"When an Application transmitting sensitive data communicates over the Internet with the Stock Brokers' systems, it should 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 the Stock Brokers' 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) should be used." (SEBI Circular dated 3rd Dec 2018). As a best practice, data sent over public network should be encrypted using Transport Layer Security (TLS) which is preferred over SSL.

AK Equities Private Limited Mumbai

22.	**Data thru web pages over Internte**
	"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 is mandatory, making the transport channel HTTP(S)." (SEBI circular dated 3rd Dec 2018)
23.	**Disable insecure network services**
	Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc. (SEBI Circular dated 3rd Dec 2018)

9.5 Implementation Responsibilities

- Designated Officer
- Network Administrators

10. Internet Security Policy

10.1 Policy Objective

- To establish adequate security controls over the access / usage of internet through the corporate network.
- Ensure that only authorised users are allowed access to the Internet.
- Ensure against malicious codes like viruses and worms
- To log and monitor the access to the internet.

10.2 Policy Scope

This policy is applicable to all the infrastructure assets which are used for the internet access like Proxy, Content Filtering Software, Network components etc. and is applicable to all users including the employees, contractors, consultants and temporary users.

10.3 Policy Statement(s)

1. Access to internet should be provided for business purpose only.
2. Procedures should be established for control over internet access.
3. All the material downloaded from internet should be screened by updated anti-virus.
4. Procedures should be established for restricting abuse of internet access by users.
5. Procedures should be established for usage of internet data card.

10.4 Detailed Procedures

#	Detailed Procedures
1.	**Access to Internet**
	Access to the Internet must be provided only to those employees who have a legitimate business need for such access. The authorization to access Internet for an individual depends on: • The nature of work that requires the User to connect to the Internet. • The sites that he / she are authorized to access the Internet.
2.	**Control over Internet Access**
	• All Internet activity must pass through Firewall so that access controls and related security mechanisms can be applied.

A.K. Equities Private Limited Mumbai

	• Internet access should be restricted to authorized individuals only. • Sites that are not related to business activities should be restricted. • Sites providing offensive / indecent content should be blocked at all times. • Access to sites providing warez/pirated softwares, multimedia content like songs, movies should be blocked. All Internet services and applications (like instant messengers, file sharing applications, etc.) which are not required for a business need must be disabled or uninstalled. If such applications are required, they should be installed after authorization by Chief Information Security Officer.
3.	**Control over Downloads**
	• All downloaded information e.g., files, documents, Email retrieval, data / FTP downloads, Active x controls, Java, Java Applets, images etc., via the Internet must be screened with updated virus detection software prior to use.
4.	**Restrictions on Users**
	• Users are not allowed to host personal sites using Organisation facilities • In case, a user discovers that he/she has connected with a web site that contains potentially offensive material, he/she must immediately disconnect from that site and report the matter to the Manager / CISO. • The ability to connect with a specific web site does not in itself imply that the user is permitted to visit that site. • The use or attempt to initiate such activities using Organisation's computing facilities or equipment leading to abusive, unethical or "inappropriate" use of the Internet are considered grounds for disciplinary, legal and/or punitive actions, including termination of employment. • At any time and without prior notice, the management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, and

AK Equities Private Limited Mumbai

	other information stored on or passing through the Organisation's Information Technology and Network. Users must not place Organisation's information or material (confidential information, internal memos, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar services, unless the Group heads and CISO have first approved the posting of such materials.
5.	**Usage of Internet Data card etc. to connect to internet**
	• The users should not use any other means like data card when they are in the office, even with the office supplied data card or any other device unless approved by the respective person.

10.5 Implementation Responsibilities

- Designated Officer
- Internet System Administrator
- The users to whom internet access is granted

11. Desktop and Laptop Security Policy

11.1 Policy Objective

- To ensure adequate control over usage of desktops and laptops.
- To protect information systems and assets through appropriate controls over usage of external media and software applications.
- To ensure that the end-user who has been allotted a desktop / laptop is made aware of his / her responsibility towards the Organisation's assets.
- To reduce the risk of theft of assets / data by maintaining secure environment.

11.2 Policy Scope

This policy is applicable to all USERs and Workstations (Desktops and Laptops)

11.3 Policy Statement(s)

1. Desktops / Laptops issued to staff or consultants remain the property of the Organisation.
2. Procedures should be established for ensuring security of desktops / laptops.
3. Installation of software on desktops / laptops should be controlled.
4. Users should return the desktop / laptop and any other asset given by the Organisation, while leaving employment.

11.4 Detailed Procedures

#	Detailed Procedures
1.	**Ownership of desktop / laptop**
	Desktops / Laptops issued to staff or consultants remain the property of the Organisation. When a desktop / laptop is allocated to a USER, the user officially assumes "custodianship" of the desktop / laptop.
2.	**Security of desktop / laptop**
	All the users must agree to take responsibility for the security of their desktop / laptop and the information it contains.
3.	**Software on desktop / laptop**

	• Users must take all reasonable steps to protect against the installation of unlicensed or unauthorized software.
	• Installation and use of unlicensed software (software piracy) is illegal and puts the Organization at significant risk of legal action.
	• Executable software must, whenever possible, be validated and approved by IT Department before being installed.
	• Unmanaged installations can compromise the IT operating environment and also constitute a security risk, including the intentional or unintentional spreading of software viruses and other malicious software.
	• Commercial software (including shareware/freeware) must -
	  ○ Be approved by respective IT head after getting an approval from CISO for installation on the workstations.
	  ○ Have a valid license for each prospective user
	  ○ Be checked for all known security risks, including malicious software
	• Desktop and laptop users must ensure they comply with data copyright requirements.

4.	**Surrender of workstation and other asset**
	Upon leaving the employ of, the user must return the workstation and every other asset.

11.5 Implementation Responsibilities

- Designated Officer
- IT Support Team

12. Virus Protection Policy

12.1 Policy Objective

The Anti-Virus Policy is designed to ensure that

- Anti-Virus Software is installed on all Servers, Personal Computers, Laptops, E-Mail Servers, Proxies and Internet gateways.
- Only licensed and authorized AV software is being used.
- Any external device should be scanned before allowing on the Network.
- An incidence response procedure is defined in case of a virus attack on the set up.

12.2 Policy Scope

This policy is applicable to all USERs and devices eligible for installation of the Anti Virus.

12.3 Policy Statement(s)

1. Procedures should be established for selection of appropriate Anti-Virus Software.
2. Procedures should be established for ensuring vendor support.
3. Anti-Virus Software should be installed on all servers and workstations.
4. Procedures should be established for Anti-Virus controls over the Development and Test environments.
5. Procedures should be established for ensuring appropriate Anti-Virus Software settings.
6. Anti-Virus Software should be installed on all mobile computing devices.
7. Procedures should be established for third party laptops connecting to the Corporate network.
8. Procedures should be established for reporting of virus infections.
9. Procedures should be established for ensuring appropriate Anti-Virus awareness among the users.

12.4 Detailed Procedures

#	Detailed Procedures
1.	**Selection of the Anti-Virus Software**
	Selection of the Anti-Virus software is a critical decision and should be taken considering the following factors. The AV Software should be able to • Be deployed from a central AV Server on all the servers, desktops, internet proxies and gateways, E-Mail servers etc. • Identify and eradicate all known viruses and their variants • Send alerts to the user and administrators about any infections • Able to get update releases in a timely manner as per the SLA Terms and Conditions. • Scan memory, floppies, removable media, USB drives, local and network drives, BIOS, e-mails and attachments, internet browsing and downloads etc. • Should have adequate controls to ensure against modifications except by the authorized AV Administrators.
2.	**Vendor support**
	The ISC should ensure that an appropriate Service Level Agreement (SLA) is entered into with the AV Vendor covering following clauses • Intimations about any virus outbreaks. • Updates / new signatures should be made available not later than one day. • Intimation about the intermediate compensating control measures to be taken before the updates / signatures for a new virus are released. • In case of a virus infection in the Corporate network, the vendor should support for eradication.
3.	**AV Software to be installed on all servers and workstations**
	The ISC should ensure that the AV software is installed on all the servers and workstations used for running the applications including all departments, the Help Desk and administrator workstations.

AK Equities Private Limited Mumbai

4.	**Controls over the Development and Test environments**
	• The Application Service Provider who is engaged in the development and maintenance must ensure that any patches, fixes, upgrades etc. released are virus free. • When delivered, these new programs should be tested for functionality as well as checked for viruses. • AV software in the test and development environments must be kept up-to-date with latest signatures.
5.	**AV Software setting**
	The AV Software settings should be as under: • Invoke automatically at the start up • The AV administrator should protect the AV software settings with a password, so that the users cannot modify them • Automatically scan the floppies, USB drives, incoming mails and attachments, internet browsing and downloads, shares etc. • All types of files to be scanned without any EXCLUSIONS. • Automatic updates should be installed from a central server. • Scheduled for scan the entire hard disk at least once a week.
6.	**AV on mobile computing devices like laptops**
	• The ISC should set up a process of installing and keeping up-to-date, the AV software on all laptops. •
7.	**Third Party Laptops**
	• Third parties should not be allowed to connect their laptops to the Corporate Network. • If it is necessary, then the laptop must be scanned for viruses with the approved AV Software before allowing on the network.
8.	**Reporting of Infection**

3K Equities Private Limited Mumbai

	The ISC should inform all users the contact details (phone Number, e-mail IDs etc.) of the identified administrators and ISC members for reporting any virus like activity.
9.	**User Education**
	The ISC should ensure that the users are given adequate training on the following • Users should use only the approved workstations and software. • Users should ensure that the AV software on their workstation is up-to-date. • Users must not attempt to change the setting of the AV software. • User must not install freeware, downloaded or unapproved software. • Users should be given training to Identify and report any abnormal activity on the workstations e.g. abnormal delay in opening files, loss of files, unusual displays on the screen, AV software displaying virus infection message on the screen etc.

12.5 Implementation Responsibilities

- Various departments
- Designated Officer
- IT Team

13. Patch Management Policy

13.1 Policy Objective

The objective of this Policy is to ensure that

- Establish adequate controls for security of the operating systems, database and webservers.
- To ensure that computer systems attached to the Corporate network are updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits. These mechanisms are intended to reduce or eliminate the vulnerabilities and exploits with limited impact to the business.

13.2 Policy Scope

This policy is applicable to all devices on which patches and fixes are required to be installed like Operating Systems, Databases, Router-Switches, Firewalls etc.

13.3 Policy Statement(s)

1. Ensure up to date patches for various systems and devices
2. Prioritization of the patches
3. Testing of patches
4. Backup before installing any patches

13.4 Detailed Procedures

#	Detailed Procedures
1.	**Ensure up to date patches for various systems and devices**
	The Administrators should ensure that patches released for various Information Assets like Applications, Web Servers, Databases, Operating Systems, Network Switches/Routers/Firewalls etc. The patch management procedures should include the identification, categorization and prioritization of patches and updates.
2. .	**Database Security Patches**
	• The 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. • It should be ensured that the latest security patches for the databases are applied at the earliest. • Normally, patches should be installed taking a scheduled downtime. • However, if there is a need to apply emergency patches, such updates may be installed even as an unscheduled activity.
3.	**Ensure up to date Webserver Security Patches**
	Ensure that the web server is up-to-date with latest patches including the SSL/TLS patches. The 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.
4.	**Ensure up to date patches for Network Devices**
	Ensure that patches released by OEM vendor for the Network devices like Switches, Routers, Firewalls etc. are studied in test environment and then installed in the production environment.

13.5 Implementation Responsibilities

- Accountability of updating patches is of respective asset owners.

14. User and Authorisation Management Policy

14.1 Policy Objective

The objective of this Policy is to ensure that

- User Management is standardized and governance controls are implemented over the Registration, Modification and De-registration of users.
- Access / authorisation should be granted to the users as per business requirements and only against approval from the designated authority.
- Users are informed about their legitimate accesses and also educated about the consequences of access violations.
- Reviews are done of the user management process.

14.2 Policy Scope

This policy covers all USERS and their authorisations

14.3 Policy Statement(s)

5. Establish controls over default users
6. Procedures should be established for user creation, modification and deletion
7. Procedures should be established for identification of dormant and inactive user ids
8. Procedures should be established for reissue of a deleted user ID
9. Procedures should be established for assigning roles and groups to users
10. The naming convention should help uniquely identify a user on the system
11. Each user Id should be uniquely identified on a system
12. Procedures should be established for control over generic user ids
13. User ID should be locked after three failed logging attempts
14. Procedures should be established for control over temporary user ids
15. User inactivity time out should be configured
16. Adequate segregation of duties should be enforced
17. Maker – Checker Controls should be established.
18. Regular review of Users and their Privileges should be carried out

AK Equities Private Limited Mumbai

14.4 Detailed Procedures

#	Detailed Procedures
1.	**Establish controls over default users**
	Many systems (Application, Database, Operating Systems, routers etc.) have default user IDs which are required for Installation / initiation and maintenance. Also many a times the passwords for these IDs are public information (e.g. user IDs and passwords for Oracle, MSSQL etc.). As a best practice, these users IDs should be disabled / deleted OR renamed and the passwords should be changed. This will help ensure that any malicious / unauthorized activity cannot be performed using the default user ID and password.
2.	**User Creation, Modification and Deletion**
	• Users of the Information Asset can be of various Types - At the broad level there would be two types of users - Administrator and a general User. For each asset like Operating System, Database, Application, Network Components, etc. there are these two types of users. • A process should be defined and implemented to ensure that any new user creation, modification or deletion is for the business purpose, documented, approved and record maintained for future reference. • A User EXIT process should be defined and implemented to ensure that the user ID is disabled / deleted when a user exits from The Organisation. • Where possible/necessary the user ID should auto-expire on a predefined date (e.g. in case of temporary users) - A deleted user ID should be disabled and then deleted after 90 days • Generally it is advisable that a deleted user ID is not PURGED but labelled as "deleted".
3.	**Identification of Dormant and Inactive User IDs**
	User Ids which are not active for 90 or more days should be identified, documented and disabled after approval. In case such IDs are to be activated, the procedures mentioned in the next section should be followed.

AK Equities Private Limited Mumbai

4.	**Reissue of a disabled User ID**
	A disabled/Inactive user ID may be re-activated if necessary, against approvals and must be enabled only for the "original user". This process should be treated at par with creation of the new user ID and all the related controls like approval, issue of first password, change of password on first logon, record keeping etc. should be followed. This activity should be logged and monitored.
5.	**Assignment of Roles and Groups**
	Various Systems (Applications, Databases, Operating System, etc.) give the users, membership of a group, category and role. This membership gives the user, various privileges to perform his / her job responsibilities. A control process should be defined and implemented while a user is given membership of group, category or assigned role. The Process should help to ensure that the privileges given to any user are for the business purpose, documented, approved and record is maintained for future reference.
6.	**Naming Convention**
	For all users on other systems (Database, Operating Systems etc.), a naming convention should be defined. The naming convention should help uniquely identify a user on the system.
7.	**Unique Identification of each user on a system**
	Each user Id must be uniquely identified on a system. One user ID should not be issued to multiple users to ensure that accountability is established.
8.	**Generic User Ids**
	As a prudent practice, creation and usage of generic user Ids for operations and management of IT should be avoided. However, there are situations where creating unique user IDs itself may result in vulnerability e.g. creating multiple user IDs with root,

AK Equities Private Limited Mumbai

	administrator, sys, system etc. privileges. There are also situations where, generic IDs are required for testing purposes. In such cases, the Custodian of the Information Asset should approve shared usage of such generic user Ids by the identified team members. The Custodian should set up systemic or compensating controls to ensure that although the user ID is Generic, controls and audit trails are available to a accurately identify the user and establish accountability for activities carried using the shared generic user ID.
9.	**Locking of a User after certain number of Failed Login Attempts**
	Only a limited number of attempts should be given for a user to login after which that ID should get locked. Generally as a good practice, after a maximum of 3 to 5 bad attempts, the user ID should be locked and should be enabled only after the Administrator enables it against a formal request from the user. The number of attempts should be decided and configured by the Asset owner taking into account the criticality. For resetting the locked ID an out-of-band channel should be used like sending a cryptographically encrypted link should be sent to the customer's registered email OR a random OTP could be sent as SMS to the customer's registered mobile OR manually by the Broker after verification of the customer's identify.SEBI has further 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.(SEBI Circular dated 3rd Dec 2018)
10.	**Temporary User Ids**
	If a user ID is created for a temporary period, its' expiry date should be entered during creation process itself. The system should automatically lock the user Id on the designated date.
11.	**User Inactivity Time Out**
	• Inactivity time out should be configured at 10 minutes. • The user should be required to enter his / her password to unlock the screen.
12.	**Segregation of Duties**

	Adequate Segregation of Duties should be enforced for conflicting duties. In cases where conflicting duties are required to be performed by the same user, adequate compensating controls like supervision, logs, dual authorisation etc. should be used.
13.	**Maker – Checker Controls (Never Alone Principle)**
	A maker-checker control should be implemented over the critical or sensitive activities done by any user e.g. creation, modification, and deletion of the user IDs, changes to the parameter files, defining new products, critical systems initialisation and configuration, PIN generation, creation of cryptographic keys, use of administrative accounts etc. Similarly, maker – checker controls should also be implemented over the transactions done by general users of the application. As a principle, one user should not be able to complete a transaction / activity end-to-end.
14.	**Review of Users and their Privileges**
	The CISO should ensure that review of Users and their Privileges is carried out at least once a year.

14.5 Implementation Responsibilities

- The Administrators of various systems like Applications, Databases, Operating Systems, Network Components, etc.
- The Department Administrators
- IT Support Team

15. Physical and Environmental Security Policy

15.1 Policy Objective

Objective of the policy is to define the requirements for protecting the information and technology resources from physical and environmental threats and reduce the risk of loss, theft, damage, or unauthorized access.

15.2 Policy Scope

This policy is applicable to all USERS and covers secure areas like server room / data centre, network closets and critical infrastructure assets like Air Conditioning Units, Power Generators, etc.

15.3 Policy Statement(s)

1. Implement Physical Access restrictions
2. Critical equipment / areas should be secured
3. Logs / Audit Trails should be enabled and reviewed regularly
4. USERS should wear Identification Badges
5. Consider Security Guards where necessary
6. Procedures for visitors access should be established
7. Implement Controls over Lost Identity Badges
8. Prohibit Piggybacking
9. Choose secure location for the Critical Secure Areas
10. Ensure security of Cables / Electrical fittings
11. Ensure Fire detection and suppression systems are operational
12. Implement Control against water damage
13. Ensure cleanliness of premises and Secure Areas
14. Procedures should be established for handling power outages
15. Physical access to supporting infrastructure should be controlled
16. Implement controls over movement of equipment
17. Ensure inventory and labelling of all devices
18. Ensure Maintenance of equipment

AK Equities Private Limited Mumbai

15.4 Detailed Procedures

#	Detailed Procedures
1.	**Implement Physical Access restrictions**
	• Areas which need physical and environmental controls should be identified. Generally this will include the server room or data centre, Network rooms, Patch Panels, Racks, Air Conditioning Units, Power Generation Units, Diesel Storage Tanks, CCTV cameras and storage etc. This may also include critical business processing areas which need specific additional security measures. • Security perimeters should be used to protect areas, which may contain information processing facilities. A security perimeter is a barrier like a wall or a controlled door or a manned reception desk. • Access to critical computing facilities should be granted only those who are authorised. • USERs / visitors must not attempt to enter restricted areas in the company premises for which they have not been granted access. • The access list authorised users should be reviewed at least once a year.
2.	**Securing critical equipment / areas**
	• All critical servers and communication equipment must be located in secured rooms to prevent tampering and unauthorized access. • Entry to the server room / data centre / Computing facilities must be restricted to authorized personnel through the use of number pads / swipe cards / biometric controls keys. A list of authorized personnel must be maintained. The request for Data Centre / Computing facilities access should be reviewed and approved by CISO / Designated Officer. • Where the entry of visitors cannot be restricted through the use of swipe cards or other means, a visitors' log must be maintained to record the visits to the server room / data centre /computing facility, including vendors and maintenance personnel. This must be authorized by the Administrator prior to the visitor's entry. Visitors

AK Equities Private Limited Mumbai

	and cleaning crew must be supervised at all times whenever they are in the server room / data centre / computing facility.
3.	**Logs / Audit Trails should be enabled and reviewed regularly**
	• The use of the number pad / swipe card / biometric control to access the server room / data centre / computing facilities must be logged and reviewed at regular intervals. • If Manual paper based registers are maintained, such registers also should be authorised and reviewed at regular intervals.
4.	**USERS should wear Identification Badges**
	Each USER must wear an identification badge to gain access to the premises. The badge must have a photo of the USER
5.	**Consider Security Guards where necessary**
	Where necessary, security guards should be stationed at the main entrance to protect against unauthorized access to the location premises. If required, the guard may be stationed for 24*7. The security guards are expected to perform following • Any material coming in or going out is backed up by appropriate challan. These tasks are performed by administration department. • Any material sent out which is returnable is appropriately recorded for return on the due date by administration department. • Each Security Guard should be given adequate training about soft skills, frisking and keeping record of the material movement. HR department should maintain appropriate record of such trainings.
6.	**Entry for visitors**
	• Ensure that each visitor entering the secure area makes an entry in Visitor's Book. • Ensure that the authorised user escorts the visitors. • Visitors Log Register should be reviewed by the Administration dept.
7.	**Implement Controls over Lost Identity Badges**
	• The security officer on intimation of lost / stolen identification badges should immediately deactivate the badge.

AK Equities Private Limited Mumbai

	• Identification badges that have been lost or stolen or are suspected of being lost or stolen must be reported to the Admin Department immediately. • Process for issuing duplicate identity badges should be started by admin department after receiving required authorisation.
8.	**Prohibit Piggybacking**
	• USERS must not permit unknown or unauthorized persons to pass through doors requiring swipe cards / number codes.
9.	**Choose secure location for the Critical Secure Areas**
	• The Critical Secure Areas should be located in buildings which are adequately strong. • To minimize theft and water damage, critical secure areas should preferably be located above the second floor in buildings and that floor should not be top floor.. • To minimize potential damage from smoke and fire, facilities like kitchen should be located away from (including not directly above or below) the critical secure areas. • Likewise, to minimize potential water damage, rest room facilities or water tanks should not be located directly above these facilities.
10.	**Ensure security of Cables / Electrical fittings**
	• Data Cables connecting computing equipment and other support equipment must be neatly organized (structured cabling). Cabling maps should be prepared. • All electrical wiring and LAN cabling must be structured and run through concealed cabling. • Electrical wiring and LAN cabling MAPs should be prepared. • Circuit breakers of appropriate capacity must be installed to protect the hardware against power surges. • Electrical mains must be properly guarded against accidental / unauthorized access. • Emergency power off switches should be located near the EXIT door to facilitate rapid power down

A.K. Equities Private Limited Mumbai

11.	**Ensure Fire detection and suppression systems are operational**
	• Smoking should be prohibited within the office premises and critical secure areas. • Smoke detectors must be placed at strategic locations to set off an alarm in case of smoke / fire. • Fire extinguishers (which are human friendly and usable over computer hardware) must be installed to minimize damage. In case of fire, activation of the extinguisher, wherever possible, should be automatic. • Smoke detectors must be placed below the raised floor and above the false ceiling of the server room / data centre. • The fire alarm, smoke detectors and extinguisher system must be inspected and tested as per vendor recommendations and at least once a year. • Training should be given to the USERs on the use of the fire extinguisher system at least once a year.
12.	**Implement Control against water damage**
	• Locations of "Secure Areas" with potential for water damage must be avoided. • There must be a master switch / valve for all water mains. • Humidity monitors should be installed in the server room / data centre to control the humidity content.
13.	**Ensure cleanliness of premises and Secure Areas**
	• The floor, walls, storage cabinets and IT equipment must be regularly cleaned. Unwanted materials such as boxes, leftover materials, cables etc. should not be kept inside the data centre. • Eating & drinking must be prohibited in the data centre • Users must ensure that their desks are clean (no confidential information should be kept in the open)
14.	**Handling power outages**

	• Adequate number of uninterrupted power supply (UPS) systems must be installed for all critical computing and supporting equipment. The UPS must have the capability to continue the power supply to allow for an orderly shutdown of the system. • In areas susceptible to outages of power for longer durations, generators should be provided to ensure working of servers and all business critical workstations. • Backup power facilities must be tested at least once a month to ensure reliable functioning of the equipment. • Emergency lighting may be provided for use during power outages.
15.	**Physical access to supporting infrastructure should be controlled**
	Access to facilities that support information processing systems, such as, the telecommunication equipment, the emergency power equipment (UPS, etc.), network hubs etc. should be subject to the same controls as advised for the Server Room / Data Centre.
16.	**Implement controls over movement of equipment**
	• It is the responsibility of IT Department / Facilities Management / administration department to effect the movement of all types of information systems equipment. Users must not relocate or remove any equipment themselves. • Appropriate passes/authorization should be issued to effect the removal of equipment from the building.
17.	**Ensure inventory and labelling of all devices**
	• A complete and up-to-date inventory of all devices should be maintained. • Each Device should be identified with the asset code for easy identification. • Workstations / Laptops must be traceable to individual users. Each individual must be made accountable for the physical security of Workstations / laptop.

AK Equities Private Limited Mumbai

	• When an incident of theft of a Workstations / laptop comes to light it must be reported by the user to the Department Head, & Head-IT and physical security department immediately.
18.	**Ensure Maintenance of equipment**
	Equipment should be maintained to ensure its continued availability and integrity. Following guidelines should be considered • Equipment should be inspected and maintained in accordance with the suppliers recommended service intervals and specifications. • Only authorized maintenance personnel should carry out repairs and service maintenance. • Appropriate controls should be taken when sending equipment off premises for maintenance. For critical devices transit insurance cover may be obtained. • Only authorised users should be allowed to take the equipment off premises • Appropriate record of movement of such equipment should be maintained for tracking purposes

15.5 Implementation Responsibilities

- Physical Security Department
- Administration Department
- IT Infrastructure Department

AK Equities Private Limited Mumbai

16. Log / Audit Trail Management Policy

16.1 Policy Objective

This Policy is developed to ensure that

- Audit Trails / Logs capture adequate details like the user ID, Activity of the user, the location identifier and the Date and Time Stamp to ensure accountability.
- System Logs should help in analysing the performance and other issues.
- Audit Trails / Logs are secured agaunauthorized modifications.
- The time stamping of logs should be done with the network time server (Clock Synchronization)
- Audit Trails / Logs should be retained for the defined period.
- A process of analysing and monitoring the logs to identify security incidents and operational problems is defined and implemented.

16.2 Policy Scope

This policy applies to all logs generated by the application systems, Database, operating systems, network components, including the physical access logs maintained in manual registers and surveillance systems.

16.3 Policy Statement(s)

1. Define Log Management Strategy.
2. Ensure that Logs capture only the necessary details.
3. Logs should not capture sensitive information
4. Ensure adequate disk space for saving logs
5. Ensure Accurate Network Date/Time Stamping.
6. Ensure Strict Access Controls over Log Files.
7. Enable Logs in Append Mode.
8. Preserve logs as per Retention Period Requirements.
9. Logs should be analysed as necessary.
10. Retain logs until completion of investigation.
11. Log host should be defined.
12. System Installation Logs should be backed up and then removed.

16.4 Detailed Procedures

#	Detailed Procedures

AK Equities Private Limited Mumbai

1.	**Define Log Management Strategy**
	• A Log / audit trail strategy should be designed, documented and implemented to help ensure that the logs are enabled, stored securely, analysed and monitored. • Audit Trails / Logs should be enabled on the Applications and supporting Infrastructure components like Databases, Operating Systems, Web Servers, Switches, Routers and Firewalls. • In case, logging degrades the performance of systems beyond acceptable limits, only selective logging and monitoring of critical commands/ activities may be configured. • Physical (Registers) or systemic (Soft) Logs / Audit Trails should be implemented for access to the critical areas like Data Centre, Power Supplies, Air Conditioning Units etc.
2.	**Ensure that Logs capture only the necessary details.**
	The logs should capture details like user Id, Location, activity and date and time to establish accountability.
3.	**Logs should not capture sensitive information**
	The logs should be configured in such a manner that they should not capture sensitive information like the Process ID (PID), biometric details, OTP, passwords (even in encrypted form) etc.
4.	**Ensure adequate disk space for saving logs**
	To ensure that logging is not disrupted, adequate disk space should be maintained all the time on respective systems.
5.	**Ensure Accurate Network Date/Time Stamping**
	To ensure correct analysis of the logs, an accurate network date/time stamping should be used. The date and time should be synced with GMT/UTC to ensure consistency across all devices.
6.	**Ensure Strict Access Controls over Log Files**
	The Log files should be access controlled to ensure against unauthorized modifications. Wherever possible, the logs should be enabled in Binary mode.

7.	**Enable Logs in Append Mode**
	Generally and wherever technically possible, Logs should be enabled in append mode, to ensure that the earlier logs are not overwritten.
8.	**Preserve logs as per Retention Period Requirements**
	Logs should be saved / retained for a period as required by the applicable regulatory body guidelines. Both successful and failed login attempts against a Customer's account may be logged for a reasonable period of time (The SEBI circular of 3 Dec 2018, has not specified retention period).
9.	**Logs should be analysed as necessary**
	• Logs help analyse and monitor the system performance, errors, security events, switching of users, login-logout, access failure, user activities, backup activities etc. • Logs generated by various Information Assets like Applications and supporting Infrastructure should be reviewed and analysed at regular intervals.
10.	**Retain logs until completion of investigation**
	In case of investigations, the log files should be preserved for the required period of investigation.
11.	**Log Host should be defined**
	The Log host should be defined and should be under the administrative control of a different group rather than the IT Administrator e.g. the log host may be under the control of Security Group to ensure segregation of duties.
12.	**System Installation Logs should be backed up and then removed**
	Installation logs should be backed up and then removed from the system, since they may contain installation user ID and passwords.

16.5 Implementation Responsibilities

- Administrators of various systems – Operating Systems, Application, Database, Routers, Firewalls etc.

17. Incident Management Policy

AK Equities Private Limited Mumbai

17.1 Policy Objective

The Incident Management Policy is designed to

- Establish a process for identification and management of incidents, problems, malfunctions and abuses.
- Provide guidance to the technical and management users to enable quick, efficient and effective recovery from Incidents or problems.
- To minimise loss from Incidents or problems.
- To carry out a root cause analysis, document and learn from the Incidents or problems and implement controls to arrest recurrence of the Incidents or problems.

17.2 Policy Scope

This policy is applicable to various information assets and to all USERS.

17.3 Policy Statement(s)

1. Identify possible Incidents and steps for recovery.
2. Training for Incident Identification
3. Ensure Incident / Problem Reporting
4. Analyse the Incident / Problem
5. Contain the Incident / Problem and remove the cause
6. Root Cause and Impact Analysis should be done
7. Implement additional / change of controls

17.4 Detailed Procedures

#	Detailed Procedures
1.	**Identify possible Incidents and steps for recovery**
	The IRT should ensure that various possible incidents or problems are studied and documented including the steps for resolution. Each possible incident or problem along with the steps should be documented and reviewed and rehearsed at regular intervals. The document should be available with the IRT.
2.	**Training for Incident Identification**
	Adequate and repeated training should be given to USERS to help them understand and identify an event / incident / problem. This would include demonstration of sirens, alarms, incorrect system behaviour, other indications etc.
3.	**Ensure Incident / Problem Reporting**
	The users should be informed about the process of incident / problem reporting, to the appropriate authority for an early resolution. If any vulnerability is identified in the off-the-shelf products, it should be reported to the respective regulatory authorities for meeting the compliance requirements, wherever applicable.
4.	**Analyse the Incident / Problem**
	Incidents / Problems should be assigned appropriate severity level. As part of incident / problem analysis, incident / problem severity levels should be determined by relevant designated staff members/asset custodians. These USERS should be trained to discern incidents / problems of high severity level. Moreover, criteria used for assessing severity levels of incidents / problems should be established and documented.
5.	**Contain the Incident / Problem and remove the cause**
	The Incident Response Team should first try to contain the Incident / Problem to ensure that the damages are minimal.

	After containment the Incident Response Team should remove the cause of the Incident / Problem. The Team should be careful to safeguard the evidences to help the investigation. The Team should monitor all the incidents / problems and ensure that the timelines for resolution are achieved.
6.	**Escalation Process should be established**
	Timeframe for resolution of Incidents / Problems should be commensurate with the severity level and corresponding escalation process should be defined to ensure timely resolution. These escalation procedures should be tested at regular intervals to evaluate effectiveness. If an Incident / Problem is likely to develop in a major crisis, senior management should be immediately informed. Thereafter, senior management should take a call about declaring disaster and taking necessary actions thereof. Intimation about such cases should also be given to customers or relevant statutory authorities if applicable. The employees / contractors and other relevant parties should not make comments or should not give any information about the incident on social media. Information to public will be given by Public Relations / Corporate Communications Department, if exists or by top management. In case of breach of regulatory requirements, legal and compliance team will take necessary action to report such incident / breach to the concerned authority.
7.	**Root Cause and Impact Analysis should be done**
	The Incident Response Team should carry out a root cause analysis of the Incident / Problem to establish the reasons of incident / problem and document the findings. Root Cause Analysis should cover the following: a. Root Cause Analysis i. When did it happen? ii. Where did it happen? iii. Why and how did the incident / problem happen?

AK Equities Private Limited Mumbai

	iv. How often had a similar incident / problem occurred over the last 3 years? v. What lessons were learnt from this incident / problem? b. Impact Analysis i. Extent, duration or scope of the incident / problem including information on the systems, resources, customers that were affected; ii. Magnitude of the incident / problem including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; and iii. Breach of regulatory requirements and conditions, if any, as a result of the incident / problem. c. Correction and Corrective Measures i. Immediate correction to be taken to address consequences of the incident / problem. Priority should be placed on addressing customers' concerns and / or compensation; ii. Measures to address the root cause of the incident / problem; and iii. Measures to prevent similar or related incidents / problems from occurring. The root cause analysis will help identify the control weaknesses in technology and processes.
8.	**Implement additional / change of controls**
	The IRT and the leader will review the root cause analysis and the weaknesses and define changes (including additional controls) to the technical and / or procedural controls to ensure against recurrence of such incidents / problems.

17.5 Implementation Responsibilities

- Administrators of various systems – Operating Systems, Application, Database, Routers, Firewalls etc.
- IT Support Team

AK Equities Private Limited Mumbai

18. Backup Management Policy

18.1 Policy Objective

- To ensure that a business requirement driven backup Strategy is defined and implemented.
- To ensure that appropriate backups of the relevant systems are available, in case of failure of the production environment.
- To ensure that the backups are tested for readability / restoration at regular intervals.
- To ensure that adequate sets of backups are taken for critical information assets and at least one set is stored at the identified off-site locations.

18.2 Policy Scope

- Backup process for servers, applications, databases, network components, and critical personal computers.
- Labelling, storage, handling and movement of backup media.
- Testing and restoration of the backup media.
- Recycling and destruction of the backup media.

18.3 Detailed Procedures

	• Owners of the information assets like application systems, operating systems, databases, network components and other information assets should identify the data to be backed up. • The information asset owners will decide appropriate backup plan, taking into consideration its importance to the business, legal requirements and technology available. The backup requirements shall be defined using below mentioned guidelines: • Name and contact details of the owner of the asset • Name and contact details of the custodian OR coordinator (appointed by the owner) of the asset for all backup related activities • New requirement / change in existing backup requirement • The details of servers / drives / folders / files to be backed up • The frequency of backups (daily, weekly etc.) • Whether local backup required (on a separate Hard Disk/Tape) • The type of backup (incremental / differential / full backup etc.) • Number of sets – One or Two • Whether storage at off site is required • State of the Database to be backed up (Cold, Hot, Export, etc.) • The retention period • Whether data needs to be encrypted or not

18.4 Implementation Responsibilities

- The Back Team of various systems – Operating Systems, Application, Database, Routers, Firewalls etc.

19. Vendor Management Policy

19.1 Policy Objective

The objective of this Policy is

- To ensure that a process for vendor selection and management is defined and implemented.
- To ensure that contracts / agreements with vendors address the Information Security requirements, as necessary.
- Set up a process for monitoring the vendor performance.
- The security requirements should be also made applicable to the users employed by the vendor.

19.2 Policy Scope

This policy covers all vendors giving support to the operations of

- The Data Centre,
- Information Assets like Hardware, Applications, databases, Network Devices, etc and
- Infrastructure devices like UPS, AC, Fire Extinguishers etc..

19.3 Policy Statement(s)

1. Procedures should be established for vendor selection.
2. Agreements are entered into with the vendor.
3. Provide for Alternate / Stand by vendor
4. Regular review of vendor contract.

19.4 Detailed Procedures

#	Detailed Procedures
1.	**Procedures should be established for vendor selection.**
	Define a vendor selection criterion which is based on a comparative analysis of techno-commercials of the proposal received from vendor. Selection of the vendor will be driven by various parameters like technical competency, compatibility with present set up, support and maintenance, past experience in the vendor in the business line, quality and security certifications by the vendor, DR readiness, financial stability, market reputation, and cost of the product/services.
2.	**Agreements are entered into with the vendor.**
	Ensure that appropriate and enforceable contracts / agreements are entered into with the vendor. Information Security Clauses, as appropriate, should be incorporated into the contracts / Agreements. An SLA should be made with the vendor and the performance should be monitored on a regular basis.
5.	**Provide for Alternate / Stand by vendor**
	Consider the possibility of service disruption due to inability of an existing vendor to continue operations or provide services. To address such contingencies viable alternatives should be proactively identified and kept on stand by.
7.	**Regular Review of Vendor Contract**
	The vendor contracts should be reviewed regularly (at least once a year or when due for renewal) for overall performance during the contract period. These reviews may also include review of policies, procedures and controls implemented by the vendor.

19.5 Implementation Responsibilities

- Department Heads
- IT Infrastructure Department
- General Administration Department

AK Equities Private Limited Mumbai

20. Security Compliance Policy

20.1 Policy Objective

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements by ensuring compliance to various policies adopted by The Organisation.

20.2 Policy Scope

This Policy applies to all USERS who use the Organisation's computing and networking resources and covers various guidelines issued by Government and regulatory bodies. Such regulatory Guidelines are listed in Annexure A. **"List of Guidelines by various Government and Regulatory Bodies".**

20.3 Policy Statement(s)

1. Identification of the applicable laws and regulatory guidelines.
2. Ensure Implementation of the identified requirements
3. Ensure Compliance with the Intellectual Property Rights
4. Comply with guidelines on E-Waste Management.
5. Protect Organisational Records.
6. Ensure Data Protection and Privacy of personal information.
7. Prevention of misuse of information processing facility.
8. Compliance with Organisation's information security policies.
9. Ensure Technical Compliance Checking.
10. Sharing of Information with SEBI
11. Systems Managed by MIIs

20.4 Detailed Procedures

#	Detailed Procedures
1.	**Identification of the applicable laws and regulatory guidelines.**
	The Compliance Department shall prepare and maintain a list of applicable laws, regulations and guidelines relating to the Information Security based on the area of operations and the applicable jurisdiction. This list shall be reviewed periodically and updated.
2.	**Ensure Implementation of the identified requirements**
	The Compliance Department shall ensure that the identified provisions are communicated to the CISO from time to time for onward communication with the respective USERS. The CISO should initiate the process of making suitable changes to the existing ISMS Documents and get them approved. The CISO will maintain version history.
3.	**Ensure Compliance with the Intellectual Property Rights**
	Ensure compliance to the IPR provisions by: • Using only The Organisation approved software. • Reviewing the Servers and Desktops / laptops for potential violations • Preventing installation of software beyond the number of permitted Licenses All users should be given awareness that they should not install any unlicensed / warez software.
4.	**Comply with guidelines on E-Waste Management.**
	• Controls as defined in the chapter on E-Waste Management Policy should be implemented.
5.	**Protect Organisational Records**
	• Appropriate controls should be implemented over the various types of Records, like paper, microfilm, electronic etc. • Data storage system should help in efficiently fetching the required data

	• Retention periods of various types of records should be defined and adhered to by respective functional / department heads.
6.	**Ensure Data Protection and Privacy of personal information**
	• The data received from clients and other critical information, should be appropriately "access controlled" • The data received from clients should be deleted once the process or required task is completed and / or its' retention period as required by the client / contract is over. • In case of repetitive and long term access requirements, the data should be held on the identified server with appropriate access controls so that only authorised users have access to it
7.	**Prevention of misuse of information processing facility**
	• Users should be given appropriate awareness training that the data or the production facilities are to be used only by the authorised users • Users should be made aware about the preventive and detective controls – like physical access controls, CCTV, supervision, warning banner while logging in, logs and audit trails, content inspection and monitoring etc. The above awareness would act as a deterrent and help avoid unauthorised access attempts
8.	**Compliance with Organisation's information security policies**
	• At least once a year, the Asset owners should perform reviews of the accesses granted to users. • If any deviation / non-compliance to the security policy is observed, they should study the root cause and define and implement correction and Corrective Action
9.	**Ensure Technical Compliance Checking**
	At least once a year technical compliance checking should be performed for the critical information assets. Systems Audits and VA-PT should be performed as described in the chapter on "ISMS Audit Policy".
10.	**Sharing of Information with SEBI**

	Quarterly reports containing information on cyber-attacks and threats 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 should be submitted to Stock Exchanges / Depositories.
11.	**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 the Stock Broker / Depository Participant. The Stock Broker / Depository Participant is exempted from applying the captioned SEBI guidelines of December 2018 to such systems offered by MIIs such as NOW, BEST, etc.

20.5 Implementation Responsibilities

- Compliance Department
- Designated Officer

21. Business Continuity Management Policy

21.1 Policy Objective

The Objective of the policy is to ensure that:

- Information assets supporting the critical business activities are identified and inventoried.
- A Business Continuity Plan is developed so that the identified information assets are available for critical business activities even during situations of interruption / disaster.
- A Team represented by cross functional businesses, is identified and adequately trained to implement the BCP.
- The BCP is tested at regular intervals and is kept up-to-date.

22.2 Policy Scope

This policy covers the identified information assets supporting the critical business activities which need continuity under abnormal situations.

22.3 Policy Statements

1. Identify the Business Continuity Team leader
2. Decide the composition of business continuity team.
3. Prepare Inventory of Processes and associated assets
4. Implement the BCP.
5. Perform regular Testing of the BCP.
6. Maintain the BCP up-to-date.
7. Maintain and update contact numbers of BC team members

22.4 Detailed Procedures

#	Detailed Procedures
1.	**Identify the Business Continuity Team leader**
	• The Business Continuity Team should be headed by the Managing Director or the Owner of the Business Continuity Plan. • The Owner should nominate an alternate team leader to take ownership of the BCP, in his absence. • The Owner should be vested with the power of declaring a disaster.

	• The Owner should be the executive owner of BC Plan and should be the BC Team leader
2.	**Decide the composition of Business Continuity Team**
	• The BC Team leader and the owner of the policy should identify a team of users drawn from various functions and departments. This team should be designated as the "Business Continuity Team".
3.	**Prepare Inventory of Processes and associated assets**
	A comprehensive inventory of the various business processes and the associated information assets (like operating systems, databases, application systems, network components etc.) and other resources and their owners, should be prepared as per the Risk Management Methodology.
4.	**Implement the BCP**
	• The selected team members should be trained in their roles and responsibilities as defined within the process
5.	**Perform regular Testing of the BCP**
	• A proper test plan should be finalized and implemented to ensure its proper functionality and training to the BC team members.
6.	**Maintain the BCP up-to-date**
	It is the responsibility of the BC Team leader and the owner of this policy to ensure that the BC Plan is regularly modified and maintained to reflect the changes in the Business Processes and the Information Technology as per the Change Management Policy.
7.	**Maintain and update contact numbers of BC team members**
	A comprehensive and up-to-date list of names, phone numbers, addresses, and contact details should be maintained and made available to the BC Team members.

22.5 Implementation Responsibilities

- BCP Team
- Departmental Heads

ANNEXURE A

List of Guidelines by various Government and Regulatory Bodies

- SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 December 03, 2018
- SEBI Circular No. SEBI/HO/MRD/DMS1/CIR/P/2019/43 March 26, 2019. This circular is for the MIIs and not the brokers. Hence the guidelines of this circular are not considered.
- E-Waste Management and Handling Rules 2011 by Ministry of Environment and Forest Notification dated 12th May 2011.

For A K Equities Pvt. Ltd.

A K Equities Private Limited Mumbai

Nimish Mehta

(Director)