

# **Cyber Security and Cyber Resilience Policy**



Version 1.3

of



**Registered Office: G-5, 4353 Madan Mohan Street  
4C Ansari Road, Darya Ganj, New Delhi – 110002**

**Version 1.3**

PREPARED BY	Approved BY	Effective Date	Next Revision Date
Name: Mrs. Archana Sahni	Name: Mr. Sudhir Kumar Singhal	01-04.2025	
Signature: 	Signature: 		

### VERSION HISTORY

VERSION #	Effective DATE	AUTHORIZED BY
1.0	First Version 01-04-2019	Mr. S K Singhal
1.1	Second Version 01-04-2021	Mr. S K Singhal
1.2	Third Version 01-04-2023	Mr. S K Singhal
1,3	Fourth Version 01-04-2025	Mr. S K Singhal

## Distribution List

#	Name of the Custodian
1	<b>Board of Directors:</b> a) Mr. S.K. Singhal b) Ms. Sadhna Singhal c) Ms. Archana Sahni
2	<b>Technology Committee:</b> a) Mr. S.K. Singhal, Managing Director b) Ms. Archana Sahni, Director & Compliance Officer c) Mr. Manish Sahni, IT Head
3	<b>Chief Information Security Officer / Designated Officer:</b> Mr. Manish Kaushik
4	<b>Any other entity authorized by the CISO / Designated Officer:</b> NA

# 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.

## **COPYRIGHT NOTICE**

**\*\*Singhal Capital Market Limited\*\***

All Rights Reserved. The contents of this document are confidential and proprietary to Singhal Capital Market Ltd and no part of this document should be reproduced, published in any form by any means, electronic or mechanical including photocopy or information storage or retrieval system nor should the material or any part thereof be disclosed to third parties without the express written authorization of Singhal Capital Market Ltd

## Contents

1. Introduction	9
2. Technology and Security Governance Policy	10
3. <del>Information Publication Security Policy</del>	15
4. Asset Management Policy	17
5. Asset Classification and Risk Management Policy	22
• Asset Classification Scheme	22
6. Risk Management Policy	24
7. Acceptable Usage Policy	27
8. Media Handling Policy	30
9. E-Waste Management Policy	33
10. Personnel Security Policy	35
11. Application Security Policy	38
12. Web Server Security Policy not applicable if Website, LAN and Internet is not available	45
13. Database Security Policy	50
14. Operating Systems Security Policy	55
15. Network Security Policy	61
16. Internet Security Policy	69
17. E-mail Security Policy – applicable only in case of clients’ own domain	72
18. Desktop and Laptop Security Policy	79
19. Security Policy for Handheld/Smart Devices	81
20. Virus Protection Policy	84
21. Patch Management Policy	88
22. User and Authorisation Management Policy – for 2 person staff broker/dp it will not be applicable	90
23. Password and Authentication Management Policy	95
24. Teleworking Policy	103
25. Encryption Policy	106

26.	Clear Desk Clear Screen Policy – for more than 5 people staff	109
27.	Capacity Management Policy	112
28.	Change Management Policy	115
29.	Physical and Environmental Security Policy – for Type I broker create a para	119
30.	Log / Audit Trail Management Policy – applicable for more than 1 back office users	125
31.	Incident Management Policy for type I & II broker make a small para	128
32.	Backup Management Policy – Type zero and I – convert it to two small para	133
33.	Business Continuity Management Policy – I & zero – $\frac{3}{4}$ small para	139
34.	Vendor Management Policy – make small para	143
35.	Security Compliance Policy	147
36.	ISMS Audit Policy	151



# 1. Introduction

**Singhal Capital Market Ltd.** is registered with NSE as a Trading Member

**Singhal Capital Market Ltd.** trades on NSE through Exchange Terminals viz., NEAT Terminals. It has only one office and has no branches. It is doing own trading and clients trading. It has 7 employees and has back-office software of Shilpi Computers Pvt. Ltd.

**This policy is based on the above facts.**

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 <broker>.

The Information Security Policies are designed as per Information Security guidelines for Stockbrokers / 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.

- **Information Security Policies and Procedures (henceforth referred to as ISPP)** - This document basically covers the security policies and procedures for areas NOT related to Information Technology. whereas **wherever needed**
- **Cyber Security and Cyber Resilience Policies and Procedures (henceforth referred to as CSCRPP)** - This document basically covers the security policies and procedures for areas relating the Information Technology.

## 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**

### **1.2.1 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.

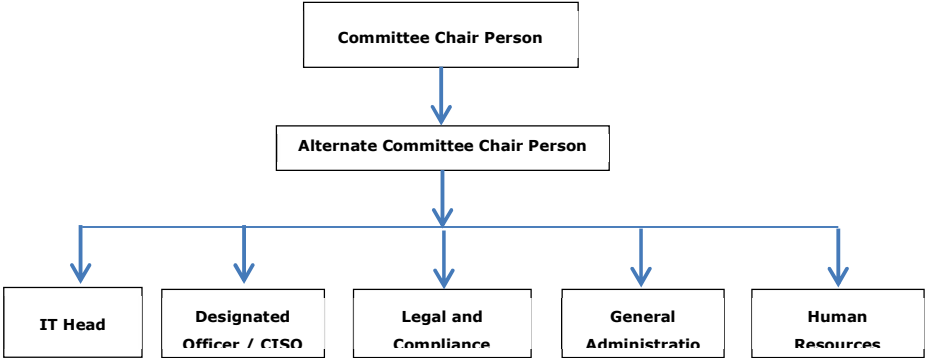
### **1.2.2 Policy Scope**

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.

### **1.2.3 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

#### 1.2.4 Detailed Procedures

#	Detailed Procedures
1.	<p><b>Set up a Technology / Strategy / Security Committee</b></p> <p>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.</p> <p>Hereinafter this committee will be referred to as "Technology Committee".</p> <p>The Organisation structure of the "Technology Committee" is as under:</p>  <pre> graph TD     A[Committee Chair Person] --&gt; B[Alternate Committee Chair Person]     B --&gt; C[IT Head]     B --&gt; D[Designated Officer / CISO]     B --&gt; E[Legal and Compliance]     B --&gt; F[General Administration]     B --&gt; G[Human Resources] </pre>
2.	<p><b>Define roles and responsibilities of The Technology Committee</b></p> <p>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.</p> <p>Roles and Responsibilities of Technology Committee Members are as under</p> <ul style="list-style-type: none"> <li>• <b>The Committee Chairperson</b> <ul style="list-style-type: none"> <li>○ To act as an official spokesperson in case of disaster and act as the contact person to media and newspaper.</li> <li>○ To support the business through strategic direction and resolving immediate business issues and challenges.</li> <li>○ To keep up with changes in business environment and map it to Information Technology Environment.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ To provide resources for raising the level of information security awareness.</li> <li>○ To approve the methodologies and processes for information security, develop road maps and strategies, prioritize the information security initiatives.</li> <li>○ To ensure compliance with the legal, regulatory and contractual obligations.</li> <li>○ To maintain a repository of all the critical passwords handed over by the information asset owners in sealed envelopes.</li> </ul> <ul style="list-style-type: none"> <li>● <b>The Alternate Committee Chairperson</b> <ul style="list-style-type: none"> <li>○ Take over as Chair Person in the absence of the normal Committee Chair Person.</li> <li>○ Perform all the functions listed for the Committee Chairperson above.</li> </ul> </li> </ul> <ul style="list-style-type: none"> <li>● <b>IT Head</b> <ul style="list-style-type: none"> <li>○ To implement the decisions taken by Technology Committee.</li> <li>○ To define roles and responsibilities for various IT Department users / teams.</li> <li>○ To keep contact with authorities, support vendors etc.</li> <li>○ To keep contact with special interest groups.</li> <li>○ Monitor and manage security incidents.</li> <li>○ To manage to People, Process, Technology.</li> <li>○ Monitoring and management of systems, administrators, IT operations, Users, Authentication and Authorisation, Anti Virus set up, backup, log / audit trail etc..</li> <li>○ To ensure that security requirements are met while acquiring or developing a new system.</li> <li>○ To ensure correct processing of the information.</li> <li>○ To handle licensing issues.</li> <li>○ To develop, implement and test Business Continuity Plan and Disaster Recovery Plan (BCP and DRP).</li> </ul> </li> </ul> <ul style="list-style-type: none"> <li>● <b>Designated Officer / Chief Information Security Officer (CISO)</b> <ul style="list-style-type: none"> <li>○ To act as the executive owner of the Information Security and Cyber Security and Cyber Resilience Policies.</li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li>○ To identify the security requirements of the organization.</li> <li>○ To manage Security Architecture.</li> <li>○ To formulate and review information security and Cyber Security and Cyber Resilience policies and procedures.</li> <li>○ 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.</li> <li>○ To perform and review Risks Assessment for Assets.</li> <li>○ 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.</li> <li>○ To record and maintain the Minutes of Technology Committee Meetings.</li> </ul> <ul style="list-style-type: none"> <li>● <b>Legal &amp; Compliance</b> <ul style="list-style-type: none"> <li>○ To identify the legal, regulatory and contractual obligations and ensure compliance with them.</li> <li>○ To establish a procedure of obtaining Non-Disclosure Agreements from USERS.</li> <li>○ Ensure timely reporting to the Regulatory Bodies like NSE, BSE, SEBI etc.</li> </ul> </li> <li>● <b>General Administration</b> <ul style="list-style-type: none"> <li>○ To ensure the physical and environmental security controls over Secure Areas (Data Centre, Air Conditioning Units, Fire Extinguishers etc. are implemented, reviewed and monitored..</li> <li>○ 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.</li> <li>○ Maintain contact details for hospitals, police, fire station etc.</li> </ul> </li> <li>● <b>Human Resources</b> <ul style="list-style-type: none"> <li>○ To ensure that security controls are practiced at the three stages of employment of any USER – Before Employment, During Employment and After Employment</li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li>○ To ensure that information security responsibilities are intimated from the stage of induction.</li> <li>○ To ensure that thorough background checks are carried out for potential employees of Singhal Capital Market Ltd. before commencement of employment.</li> <li>○ To establish a procedure of obtaining Non-Disclosure Agreements from employees.</li> <li>○ To impart Security &amp; Process training and job profile awareness training.</li> <li>○ To ensure proper segregation of duties.</li> <li>○ 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.</li> </ul> <p>Based on point1 change this point</p>
<b>3.</b>	<b>Define frequency for meeting of Technology Committee</b>
	<p>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.</p> <p>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 3<sup>rd</sup> Dec 2018)</p>
<b>4.</b>	<b>Keep record of the Minutes of Meetings.</b>
	<p>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.</p>
<b>5.</b>	<b>Reporting to SEBI about the status of implementation</b>
	<p>The Designated Officer / CISO should communicate to SEBI, the status of implementation of the provisions of the circular dated 3<sup>rd</sup> Dec 2018, in their monthly report</p>

### 1.2.5 Implementation Responsibilities

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

### **3. Information Publication Security Policy**

#### **1.2.1 Policy Objective**

To ensure that any information that is made available to the public through printed (e.g. brochures) or electronic means (e.g. web site, marketing clips etc.) is against appropriate authorisation is controlled for Integrity.

#### **1.2.2 Policy Scope**

This Policy applies to all user (including contractors, consultants, third party associates etc.) who use the computing and networking resources of the Organisation.

The Policy applies to any information which is made public through any means like oral, electronic, paper, web based, films, etc.

#### **1.2.3 Policy Statement(s)**

6. Procedures should be established for authorisation of information
7. Matrix for authorisation of information before publishing it should be prepared
8. Appropriate awareness trainings should be given to custodians of information
9. Appropriate awareness trainings should be given to Help Desk
10. Guidelines for publishing information should be established

#### 1.2.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Authorisation of Information</b>
	Before any information is made public, it should be reviewed and approved for contents, formatting, compliance to the security policy, legal compliance etc.
2.	<b>Authorisation Matrix</b>
	Appropriate authorisation must be obtained before publishing it. The Authoriser/s should study the information from various angles and understand the risk if it is accessible to / falls into the hands of unintended audience.
3.	<b>Awareness to the custodian</b>
	During operations / processing the information may be handled by various users. These users are "Custodians" and have access to the classified information. Hence it is necessary that these "Custodians" should be given appropriate awareness training with respect to handling the information.
4.	<b>Awareness to the Help Desk</b>
	The Help Desk function should be given appropriate training. The Help Desk team should have a repository of standard set of questions and answers so that unnecessary information is not passed out
5.	<b>General Guidelines for publishing information</b>
	<ul style="list-style-type: none"><li>• It should not provide any details concerning the organisation's security.</li><li>• It should not contain personal information (such as bio data, contact details etc.) except where necessary and approved for the purpose.</li><li>• The information should be reviewed with respect to its possible abuse</li><li>• Check if the information "to be published" can be used along with the "information already public" to deduce critical information</li><li>• Does the information make the URL / web site / other locations attractive for attacks?</li></ul>

#### 1.2.5 Implementation Responsibilities

- All users of The Organisation



## **4. Asset Management Policy**

### **3.1.1 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.

### **3.1.2 Policy Scope**

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

### **3.1.3 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.

### 3.1.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Controls over procurement of IT Assets and Services.</b>
	<p>All information assets should be procured after receiving proper requisition in writing from the respective department heads.</p> <p>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.</p> <p>Where necessary, multiple quotations would be sought and comparison / negotiations would be carried out before placing the order for procurement.</p>
<b>2.</b>	<b>Maintain up-to-date information asset inventory register.</b>
	<p>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.</p> <p>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.</p>
<b>3.</b>	<b>Information assets should be tagged / labelled appropriately.</b>
	<p>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.</p>
<b>4.</b>	<b>Optimal utilization of IT Assets and Services should be ensured</b>
	<ul style="list-style-type: none"> <li>• Information assets should be used only for official purpose.</li> <li>• 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.</li> <li>• Any changes / modifications to settings / configuration of information assets should be carried out by authorised and qualified personnel only.</li> </ul>
<b>5.</b>	<b>Assets should be properly maintained.</b>
	<ul style="list-style-type: none"> <li>• All the information assets should be maintained as per recommendations of the respective Original Equipment Manufacturer (OEM).</li> </ul>

	<ul style="list-style-type: none"> <li>• Appropriate records for maintenance of information assets should be kept.</li> </ul>
<b>6.</b>	<b>Assets should be adequately insured</b>
	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.
<b>7.</b>	<b>Security of Information Assets during operations</b>
	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.
<b>8.</b>	<b>Controls over Movement of Assets</b>
	<ul style="list-style-type: none"> <li>• When any information asset is in transit, then the personnel carrying the same should be responsible for its security.</li> <li>• 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.</li> <li>• Packaging should be adequate to protect the contents from any physical damage.</li> <li>• Record of all in-transit information assets should be maintained.</li> </ul>
<b>9.</b>	<b>Controls over Retirement of Information Assets</b>
	<ul style="list-style-type: none"> <li>• 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).</li> <li>• Generally, the information assets should be replaced, when they become a hindrance in the performance of day-to-day activities.</li> <li>• 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.</li> <li>• 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.</li> </ul>

	<ul style="list-style-type: none"> <li>Once the information asset is replaced, the IT Department should remove the old information asset and start the disposal process.</li> </ul>
<b>10.</b>	<b>Controls over Disposal of Information Assets</b>
	<ul style="list-style-type: none"> <li>All the information assets should be disposed securely and safely when no longer required.</li> <li>In case of records like paper documents, the same should be destroyed using a paper shredder after the prescribed period of time</li> <li>In case of disposal of IT equipment, the information / data should be irreversibly deleted before the equipment is disposed off.</li> </ul> <p>For more details on disposal of IT equipment, please refer policy on E-Waste Management Policy</p>

### **3.1.5 Implementation Responsibilities**

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

## 5. 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.

#### **CLASSIFICATION 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 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

## 6. 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.

### 1.1 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: <ul style="list-style-type: none"><li>• Asset Name/Hostname</li><li>• Asset Type</li><li>• Asset Description</li><li>• Asset Custodian</li><li>• Asset / Risk Owner</li><li>• CIA Values</li></ul>
3.	<b>C-I-A Values</b>	The CIA Values shall determine criticality of the asset.



	Defining the Criticality of the Asset	<p>a)Confidentiality - Ensuring that access to information is appropriately authorized.</p> <p>b)Integrity - Safeguarding the accuracy and completeness of information and processing methods</p> <p>c)Availability - Ensuring that authorized users have access to information whenever required.</p> <p>These values can be 1, 2 or 3.</p> <p>Asset criticality shall be defined as:</p> <ul style="list-style-type: none"> <li>• Asset will be classified as Non-Critical (1) if all three CIA values are "1".</li> <li>• Asset will be classified as Moderately Critical (2) if any of the CIA value is "2".</li> <li>• Asset will be classified as Critical (3) if any one of the CIA value is "3".</li> </ul>
4.	<b>THREAT Value</b> 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.	<b>INITIAL IMPLEMENTATION Value</b> Implementing controls to mitigate the threats	<p>This status of control implementation will carry a value as follows:</p> <ul style="list-style-type: none"> <li>• If a control is already implemented, the value will be "1".</li> <li>• If a control is not implemented, the value will be "2".</li> </ul>
5.	<b>VULNERABILITY Value</b> Identifying the Vulnerabilities	<p>If a control is not implemented to mitigate a threat, it results in a vulnerability. This vulnerability shall be evaluated as follows:</p> <ul style="list-style-type: none"> <li>• If a control is implemented, the value of vulnerability will be 1.</li> <li>• If a control is not implemented, the value of vulnerability will be 3.</li> </ul>
6.	<b>INITIAL RISK VALUE</b> Calculating the Initial Risk Factor and defining the threshold for acceptable risk.	<p>For calculating the "<b>Initial Risk factor</b>" for each control, the values of Asset Criticality, Threat Impact, status of Control Implementation and Vulnerability will be multiplied.</p> <p>The Organization has accepted that any risk factor which is <i>equal to 18 or higher</i> deserves Implementation of Risk Treatment Plan. Any value which is less than 18 is accepted as "Business Risk"</p>

7.	<b>RTP or EXCEPTION</b> 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 <i>equal to 18 or higher</i> . Appropriate reasons and with approval details shall be documented.
8.	<b>REVISED RISK VALUE</b> 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.

## **7. Acceptable Usage Policy**

### **3.2.1 Policy Objective**

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

### **3.2.2 Policy Scope**

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

### **3.2.3 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.

This will purely be depended on the size of the company – of 2-3 people not needed – else required.

### 3.2.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Information assets to be used for official purpose.</b>
	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.
<b>2.</b>	<b>Every USER should adhere to the Policies and Procedures.</b>
	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.
<b>3.</b>	<b>Prudent limited personal usage is permitted.</b>
	<p>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.</p> <p>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.</p> <p>Final judgement about whether the "personal usage" was "limited" or not would be with the management.</p> <p>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.</p>
<b>4.</b>	<b>Information Assets should be monitored for policy compliance.</b>
	USERS should understand that the Information Assets are subject to being monitored including the personal data, emails and internet logs.
<b>5.</b>	<b>Installations and Configurations by Authorised USERS only</b>
	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.
<b>6.</b>	<b>Users to take reasonable measures to protect the equipment</b>
	Users should take reasonable precautions and measures to secure the equipment provided to them as they would take for their own assets.

### 3.2.5 Implementation Responsibilities

- IT Support Team
- All USERS

## **8. Media Handling Policy**

### **3.3.1 Policy Objective**

The objective of the policy is to

- Ensure that information media is controlled and physically protected.
- Ensure that all media is stored in a safe, secured environment in accordance with manufacturers' specifications
- Develop procedures for secure and safe disposal of media to minimize the risk of sensitive information leakage to unauthorized persons
- Develop procedures for handling, storing, and communicating information consistent with its classification.

### **3.3.2 Scope of the Policy**

The policy applies to various removable media used like External (portable) Hard Disks, Backup Tapes, USB devices, CDs etc. and paper documents. and is applicable to all USERS involved in handling removable media.

### **3.3.3 Policy Statement**

1. Portable Media should be appropriately labelled.
2. Controls over Portable media usage.
3. Controls over media in transit.
4. Controls for storage of media.
5. Procedures for disposal of media.

### 3.3.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Portable Media should be appropriately labelled.</b>
	All types of media like portable hard disks, Backup Tapes, CDs, should be appropriately labelled to help correctly identify the media.
2.	<b>Controls over Portable media usage</b>
	<ul style="list-style-type: none"><li>• All the media should be stored in the safe and secure environment</li><li>• Appropriate authorisation shall be taken from respective department head for using removable media such as CD, Pen Drives on a system.</li></ul>
3.	<b>Controls over media in transit</b>
	<ul style="list-style-type: none"><li>• In case of computer media or any other important document of the organization is in transit, then the personnel carrying the same should be responsible for its security.</li><li>• 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.</li><li>• Packaging should be adequate to protect the contents from any physical damage.</li><li>• Record of all such media in transit should be maintained.</li><li>• In case where necessary, insurance cover may be obtained for media in transit.</li></ul>
4.	<b>Controls over Storage of media</b>
	<p>While storing the media, vendor recommendations should be considered like cleanliness, temperature, etc.</p> <p>The media and documents should be stored securely for the retention period as per the regulatory requirements.</p>
5.	<b>Controls over Disposal of Media</b>
	<ul style="list-style-type: none"><li>• Media should be disposed securely and safely when no longer required.</li><li>• In case of records like paper documents, the same should be destroyed using a paper shredder after the prescribed period of time</li><li>• In case of disposal, the electronic media containing the data/information should be irreversibly deleted before the equipment is moved off the site.</li></ul>

### 3.3.5 Implementation Responsibilities

- Backup Administrators

- Department USERS
- IT Support Team



## 9. E-Waste Management Policy

### 3.4.1 Policy Objective

The Electrical and Electronic Equipment containing substances like lead, cadmium, mercury, and polyvinyl chloride are hazardous to human health and environment. If such e-waste is not disposed properly, it causes harm to the environment. Thus, it is very essential to implement E-Waste management policy for protection of environment.

The objective of the policy is to:

- Reduce generation of E-Waste
- Establish procedures to ensure environmentally sound recycling of E-Waste
- Establish procedures to ensure environmentally sound disposal of E-Waste

### 3.4.2 Scope of the Policy

This policy shall cover collection and disposal of e-waste.

### 3.4.3 Definitions

- a) **"Act"** means Environment (Protection) Act, 1986 (29 of 1986).
- b) **"Disposal"** means any operation which does not lead to recycling, recovery or reuse and includes physio-chemical or biological treatment, burn it to ashes and deposition in secured landfill.
- c) **"Electrical and Electronic Equipment/ EEE"** means equipment which is dependent on electric current or electro- magnetic fields to be fully functional as specified in Schedule I as per the Rules (Refer Annexure I).
- d) **"e-waste"** means electrical and electronic equipment, whole or in part, which are intended to be discarded.
- e) **"Producer"** means any person who manufactures and offers to sell Electrical and Electronic Equipment under his own brand, or offers to sell assembled Electrical and Electronic Equipment produced by other manufacturers or suppliers under his own brand, or offers to sell imported Electrical and Electronic Equipment.

### 3.4.4 Policy Statements

1. Controls should be established for identifying E-Waste
2. Controls over E-Waste for recycling or buy-back arrangements.
3. Maintain Security and Record of E-Waste

### 3.4.5 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Controls should be established for identifying E-Waste</b>
	<ul style="list-style-type: none"><li>• Appropriate precautions should be taken for identification of E-Waste. e.g. Desktop, Laptop, Server Hardware, Printer, Cartridges, Media Tapes, Internal/External Hard Drives, USB Devices etc.</li><li>• Maintain and review the inventory of all E-Waste material to be sold / disposed.</li><li>• Necessary authorisation shall be obtained from respective person.</li></ul>
<b>2.</b>	<b>Controls over E-Waste for recycling or buy-back arrangements</b>
	<ul style="list-style-type: none"><li>• In case the E-Waste Management is outsourced, it should be ensured that the vendor is a government authorised entity having necessary licenses / certifications. Selection of the vendor should be done as per the supplier management policy in this document.</li><li>• In cases of buy-back arrangements with the OEM or reseller, obtain an undertaking from the “producer” that he will handle the E-waste in a manner as prescribed by the captioned Act.</li><li>• Obtain a confirmation from the selected vendor detailing the items bought / received for disposal.</li></ul>
<b>3.</b>	<b>Maintain Security and record of E-Waste</b>
	<ul style="list-style-type: none"><li>• In case of e-Waste containing data, it should be ensured that the data is not compromised. In case there is data, it shall be properly backed up and e-Waste shall be formatted and other appropriate measures (e.g. Degaussing) shall be taken before handing it over.</li><li>• Maintain record of E-Waste disposal.</li></ul>

### 3.4.6 Implementation Responsibilities

- Administration
- IT Support Team

## **10. Personnel Security Policy**

### **5.1.1 Policy Objective**

The objective of this policy is to establish procedures to select USERS with good knowledge, educational qualifications, experience, integrity, reliability and character.

### **5.1.2 Policy Scope**

This policy is applicable to all USERS who use the Information Processing assets of the Organisation and help in business operations. As already defined in Glossary, USERS include staff and non-staff users including temporary and short term users.

### **5.1.3 Policy Statement(s)**

1. Pre-employment checks should be performed
2. Ensure that Non-Disclosure Agreements are executed
3. Ensure that Conflicts of interest are avoided
4. Ensure that Conflicts of interest are avoided
5. Appropriate Security Awareness to USERS at various levels
6. Technical Competence Training to Senior / Middle Management
7. Ensure Return of Assets - Termination / Resignation

#### 5.1.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Pre-employment checks should be performed</b>
	It is the responsibility of the HR department to formulate a procedure of carrying out detailed pre-employment checks of short-listed candidates, and verify that candidates have the necessary credentials for employment. In performing these checks, it should become clear whether applicants have concealed important information about themselves. Depending on the role, the HR department should perform other checks in order to assess an individual's knowledge, educational qualifications, experience, integrity, reliability and character. These checks would also include face-to-face interviews and personality trait identification.
<b>2.</b>	<b>Ensure that Non-Disclosure Agreements are executed</b>
	All USERS should sign a Non-Disclosure Agreement. This agreement should be signed before commencement of engagement.
<b>3.</b>	<b>Ensure that Conflicts of interest are avoided</b>
	The USERS should be asked to declare any "conflicts of interest" to minimize harm of information assets and reputation. E.g. while engaging any USER in the Audit department, the HR Department should ensure that the individual has not worked in the area of operations which he is going to audit.
<b>4.</b>	<b>Ensure that a Disciplinary Process is implemented</b>
	HR Department should have a disciplinary process in place for violation of the organization's cyber and information security policies and procedures and any other information security breaches.
<b>5.</b>	<b>Appropriate Security Awareness to USERS at various levels</b>
	<p>Appropriate awareness training in layman language should be given to the users, about Cyber Security and Information Security Policies and Procedures.</p> <p>Special trainings should be organised for the senior management level users to help them understand their role in Information Security.</p> <p>Contents of such trainings should be reviewed at least once a year and should be approved by the CISO. Such trainings should be given at least once a year to all the users including existing and new employees as well as outsourced staff and vendor resources.</p>
<b>6.</b>	<b>Technical Competence Training to Senior / Middle Management</b>
	HR Department in consultation with IT Department should conduct periodic assessment of the IT training requirements for senior and middle management to ensure that sufficient, competent and capable human resources are available.

	Based on the findings of such assessments, necessary trainings should be organised for senior and middle management.
<b>7.</b>	<b>Ensure Return of Assets - Termination / Resignation</b>
	<ul style="list-style-type: none"> <li>• The HR department should establish a clearance process to ensure that when an employee resigns, all physical access codes are deactivated or changed and badges, keys, etc. are returned before the employee leaves the premises.</li> <li>• Depending on the nature of the termination, the former employees should be subject to varying levels of observation and escort. All materials that an employee wishes to remove from the premises should be inspected.</li> <li>• Employees are equally responsible for returning all badges, keys or other materials on termination of service.</li> </ul>

#### **5.1.5 Implementation Responsibilities**

- Human Resource Department
- All USERS

# 11. Application Security Policy

## 6.1.1 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.

## 6.1.2 Policy Scope

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

## 6.1.3 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.
11. Procedures should be established for certification of core business functionalities.

12. Procedures should be established for User Management Controls.
13. Procedures should be established for Authentication Management Controls.
14. Procedures should be established for Password Controls.
15. Procedures should be established for Log Management Controls.
16. Procedures should be established for Change Management Controls.
17. Procedures should be established for Incident Management Controls.
18. Procedures should be established for Capacity Management Controls.
19. Procedures should be established for Backup Management Controls.

#### 6.1.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>The Administrator – Roles and Responsibilities</b>
	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.
<b>2.</b>	<b>Asset Inventory to be maintained</b>
	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.
<b>3.</b>	<b>Controls over Installation kit</b>
	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.
<b>4.</b>	<b>Only the required components to be Installed</b>
	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.
<b>5.</b>	<b>Controls over Integrity of the System</b>
	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.
<b>6.</b>	<b>Input, Processing and Output Controls</b>
	Various types of "Input, Processing and Output Controls" should be defined, designed, developed, implemented and tested during the User Acceptance Testing as under
	<b>Input Controls</b>
	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.



	<p><b>Processing Controls</b></p> <p>During processing of various inputs, the Application should be designed to exercise adequate controls. E.g.</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Errors should be handled appropriately</li> <li>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.</li> </ol>
	<p><b>Output Controls</b></p> <ul style="list-style-type: none"> <li>• On the client terminals, only the extremely essential sensitive data should be displayed.</li> <li>• 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.</li> <li>•</li> </ul> <p>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.</p> <p>Appropriate controls should be implemented to ensure that these outputs are not abused OR cannot be accessed by unauthorized users</p>
7.	<p><b>Controls over Interfaces and Intermediate Files</b></p>
	<p>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.</p> <p>The interface scripts should not embed database connection strings and should be access controlled against unauthorised modifications.</p>

	<p>The interface scripts should have an inbuilt mechanism of checking integrity at the time of each execution, to ensure against unauthorised changes.</p> <p>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.</p>
<b>8.</b>	<b>User Acceptance Testing</b>
	The Application should be tested for business functionality and security before it is moved into production environment.
<b>9.</b>	<b>Controls over scripts developed outside of the Application</b>
	<p>Any scripts which are developed outside of the Application for additional functionality should be tested, documented and integrity control maintained.</p> <p>Further access these scripts should be controlled on the Operating Systems and / databases.</p>
<b>10.</b>	<b>Controls for securing critical systems</b>
	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul>
<b>11.</b>	<b>Implement strict Access Controls</b>
	<p>Implement strict data access controls over USERS, irrespective of their responsibilities, technical or otherwise.</p> <p>However, in certain cases it may not be possible to restrict access (e.g. Administrators and developers), then take strict measures to limit the number of such USERS with direct access,.</p>

	Furthermore activities of such privileged USERS should be logged and monitored.
<b>12.</b>	<b>API Based Terminal / Depository Participant</b>
	<p>"The Cyber Security Policy of Stock Brokers trading through APIs based terminal / Depository Participants should consider the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time." (SEBI circular dated 3<sup>rd</sup> Dec 2018)</p> <p>The Organisation should consider obtaining confirmation from the API based Application vendor in this respect.</p>
<b>13.</b>	<b>Certification of off-the-shelf products</b>
	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.
<b>14.</b>	<b>User Management Controls</b>
	Please refer to the "User and Authorisation Management Procedures"
<b>15.</b>	<b>Authentication Controls</b>
	Please refer to the "Authentication Management Procedures"
<b>16.</b>	<b>Password Controls</b>
	Please refer to the "Password Management Procedures"
<b>17.</b>	<b>Log Management Controls</b>
	Please refer to the "Log Management Procedures"
<b>18.</b>	<b>Change Management Controls</b>
	Please refer to the "Change Management Procedures"
<b>19.</b>	<b>Incident Management Controls</b>
	Please refer to the "Incident Management Procedures"
<b>20.</b>	<b>Capacity Management</b>
	Please refer to the "Capacity Management Procedures"
<b>1.</b>	<b>Backup Management Controls</b>

	Please refer to the "Backup Management Procedures"
--	--

#### **6.1.5 Implementation Responsibilities**

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

## **12. Web Server Security Policy not applicable if Website, LAN and Internet is not available**

### **6.2.1 Policy Objective**

- To ensure that the web servers (intranet and internet facing) are configured for security as per the business, Applications and Security requirements.
- Various services made available to the users are controlled and are as per the business, Application and Security requirements.
- Traffic to and from the web servers is secured as per the business and Application requirements.

### **6.2.2 Policy Scope**

This policy is applicable to all web servers and various services that may be made accessible to the users over intranet and internet.

### **6.2.3 Policy Statement(s)**

1. Procedures should be established for installation of web servers
  2. Web servers should be checked for any default / built-in user accounts before moving into production environment
  3. All the unnecessary Services should be disabled on the web servers
  4. Access to web server root directory should be restricted
  5. Default files should be removed from the web servers
  6. Appropriate error messages should be configured on the web servers
  7. Directory surfing should be disabled from the web browsers
  8. Web servers should be configured for an appropriate inactivity time-out
- Concurrent connections on the web servers should be defined as per the business requirements
9. Proper hardening of web servers should be ensured
  10. Caching of confidential information should be forbidden on web servers
  11. Confidential information should not be hard coded on the web servers and source code viewing should be disabled
  12. Websites should provide a warning message which will indicate that user is getting redirected
  13. Web servers should be protected against DOS attacks
  14. Appropriate encryption should be implemented on the web servers.
  15. Procedures should be established for User Management Controls.
  16. Procedures should be established for Authentication Management Controls.

17. Procedures should be established for Password Controls.
18. Procedures should be established for Log Management Controls.
19. Procedures should be established for Change Management Controls.
20. Procedures should be established for Incident Management Controls.
21. Procedures should be established for Capacity Management Controls.
22. Procedures should be established for Backup Management Controls.

#### 6.2.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Installation of Web Servers</b>
	Web servers should be installed on a non-system partition / drive.
<b>2.</b>	<b>Rename / securely configure the default accounts</b>
	Before moving the web server into production environment, the web server should be checked for any default / built-in user accounts. These accounts are the first target for the attackers. Ensure that these default / built-in users' accounts are renamed to unique and obscure names.
<b>3.</b>	<b>Disable all unnecessary Services</b>
	Any Unused and unnecessary services like ftp, telnet, SMTP etc. should be turned off on the host machine.
<b>4.</b>	<b>Control over web server root directory</b>
	The permissions of Web Server root directory should be restricted only to web-server administrators.
<b>5.</b>	<b>Control over default files</b>
	All non-required default files which are installed on the web-server should be removed before moving the web-server into production environment.
<b>6.</b>	<b>Control over Error Messages</b>
	Web server should be configured to display generic error messages. Default error messages should be customized to hide confidential and unnecessary details which can be displayed to the users.
<b>7.</b>	<b>Control over Directory Surfing</b>
	Directory surfing should be disabled so that a user is not able to enumerate various paths and files inside the web-server.
<b>8.</b>	<b>Inactivity Time Out</b>
	The web server should be configured for an appropriate time out if the user remains inactive for a certain number of minutes.
<b>9.</b>	<b>Control Over Concurrent connections</b>
	Web Server should be configured for a definite number of concurrent connections as per the business requirements.
<b>10.</b>	<b>Hardening of Web-server.</b>
	Web Server should be hardened and required registry modifications should be made as per the hardening guidelines.
<b>11.</b>	<b>Control over Caching</b>

	Caching of confidential information must be forbidden on web server and clients
<b>12.</b>	<b>Control over View Source</b>
	IP address, password should not be hard coded and 'view source' option should be disabled.
<b>13.</b>	<b>Warning about Links to other web sites</b>
	Third party URLs (redirection) on the Websites should provide a warning message which will indicate that user is getting redirected
<b>14.</b>	<b>Protection against DOS attacks</b>
	Ensure that appropriate limits are set on the bandwidth usage, "connection time out" and "limit number of concurrent connections" to protect against Denial Of Service (DOS) attacks.
<b>15.</b>	<b>Control over Communication Security (SSL/TLS Encryption)</b>
	Since SSL is now deprecated, TLS V1.1 or higher should be used for encrypting web traffic. Wherever possible, it is recommended to use strong encryption ciphers such as RSA, ECDH etc.
<b>16.</b>	<b>User Management Controls</b>
	Please refer to the "User and Authorisation Management Procedures"
<b>17.</b>	<b>Authentication Controls</b>
	Please refer to the "Authentication Management Procedures"
<b>18.</b>	<b>Password Controls</b>
	Please refer to the "Password Management Procedures"
<b>19.</b>	<b>Log Management Controls</b>
	Please refer to the "Log Management Procedures"
<b>20.</b>	<b>Change Management Controls</b>
	Please refer to the "Change Management Procedures"
<b>21.</b>	<b>Incident Management Controls</b>
	Please refer to the "Incident Management Procedures"
<b>22.</b>	<b>Capacity Management</b>
	Please refer to the "Capacity Management Procedures"
<b>23.</b>	<b>Backup Management Controls</b>
	Please refer to the "Backup Management Procedures"

### 6.2.5 Implementation Responsibilities



- Web Server Administrators

## **13. Database Security Policy**

### **6.3.1 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.

### **6.3.2 Policy Scope**

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

### **6.3.3 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
14. Procedures should be established for User Management Controls.
15. Procedures should be established for Authentication Management Controls.
16. Procedures should be established for Password Controls.
17. Procedures should be established for Log Management Controls.
18. Procedures should be established for Change Management Controls.
19. Procedures should be established for Incident Management Controls.
20. Procedures should be established for Capacity Management Controls.
21. Procedures should be established for Backup Management Controls.

#### 6.3.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Database Ownership</b>
	<ul style="list-style-type: none"><li>• The Application Owner should be responsible for confidentiality, integrity and availability of the Database.</li><li>• The Application Owner should ensure that the Operating System on which the Database has been installed is appropriately secured.</li></ul>
2.	<b>Procedures for Database installation and Upgrade</b>
	<ul style="list-style-type: none"><li>• Identify, document and test the security features of the Database before installation to the production sites.</li><li>• 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.</li><li>• Define and implement the security controls for the Database</li><li>• As a best practice the database should be installed in a separate drive / folder, segregating it from the application program files.</li></ul>
3.	<b>Control over access to Database</b>
	<ul style="list-style-type: none"><li>• OS level file and directory permissions should be restricted and the access should be given "On Need" basis.</li><li>• Access to database records and related files for users should be restricted through application only.</li><li>• 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.</li><li>• Users should be created on the DB only "On Need" basis, with restricted permissions, and granting of privileged rights should be avoided.</li><li>• System and Database Administrator roles should be segregated. Ensure that the built-in-administrator is not a member of the "sysadmin" roles.</li><li>• Command prompt on the SQL server should be disabled, if not required</li></ul>
4.	<b>Databases must be monitored regularly</b>

	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.
<b>5.</b>	<b>Transaction logs monitoring</b>
	Transaction logs disk space should be continuously monitored.
<b>6.</b>	<b>Critical database mirroring</b>
	Critical databases should be mirrored on separate disks for recovery from system, file, or component failure.
<b>7.</b>	<b>Backup / Recovery procedures</b>
	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.
<b>8.</b>	<b>Security of database</b>
	<ul style="list-style-type: none"> <li>• To ensure integrity of the production database, it should be segregated from the test and development database.</li> <li>• 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.</li> <li>• Access to data stored on tape backups, data mirrors or any derived exported data should be restricted by using appropriate security controls.</li> <li>• 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.</li> <li>• If feasible, default port numbers for databases should be changed.</li> </ul>
<b>9.</b>	<b>Controls over scheduled jobs</b>
	<ul style="list-style-type: none"> <li>• Job Scheduling should be granted to only selected users.</li> <li>• Scheduled jobs should be periodically monitored.</li> </ul>
<b>10.</b>	<b>Segregation development-test and production environments</b>
	<ul style="list-style-type: none"> <li>• Production environment should be kept separate from the test and development environment.</li> <li>• The production environment should not be populated into test or development environment without adequate sanitization.</li> </ul>
<b>11.</b>	<b>Password not be stored in script/configuration files</b>

	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Field level data like passwords should be encrypted, taking into consideration the business, technical, regulatory and contractual requirements.</li> </ul>
<b>12.</b>	<b>Stored procedures, functions and triggers to be encrypted</b>
	Stored procedures, functions and triggers should be encrypted on the production environment.
<b>13.</b>	<b>Password for Application Systems</b>
	<p>Passwords for Application Systems should be stored in the database in an encrypted form only.</p> <p>Wherever possible, the Application User ID should be integrated with the Active Directory.</p>
<b>14.</b>	<b>User Management Controls</b>
	Please refer to the "User and Authorisation Management Procedures"
<b>15.</b>	<b>Authentication Controls</b>
	Please refer to the "Authentication Management Procedures"
<b>16.</b>	<b>Password Controls</b>
	Please refer to the "Password Management Procedures"
<b>17.</b>	<b>Log Management Controls</b>
	Please refer to the "Log Management Procedures"
<b>18.</b>	<b>Change Management Controls</b>
	Please refer to the "Change Management Procedures"
<b>19.</b>	<b>Incident Management Controls</b>
	Please refer to the "Incident Management Procedures"
<b>20.</b>	<b>Capacity Management</b>
	Please refer to the "Capacity Management Procedures"
<b>21.</b>	<b>Backup Management Controls</b>
	Please refer to the "Backup Management Procedures"

### 6.3.5 Implementation Responsibilities

- Manager – IT Service

- Chief Technology Officer

## **14. Operating Systems Security Policy**

### **6.4.1 Policy Objective**

Establish adequate controls for the security of the operating systems and to ensure that they are duly protected against misuse and / or unauthorized access. This Policy is designed to ensure that

- Integrity of the Operating System is ensured.
- Access to the files, folders and other system utilities is controlled.
- Access to the operating system is controlled, logged, monitored and analysed.
- The Operating System is adequately protected against the threats of viruses and malwares.

### **6.4.2 Policy Scope**

This policy is applicable to all server and workstation Operating Systems and is applicable to all USERS.

### **6.4.3 Policy Statement(s)**

1. Procedures should be established for installation of operating systems
2. Minimum Baseline Security Standards or hardening standards for all Operating Systems and critical applications should be defined, implemented and recorded
3. Access to operating systems should be restricted
4. Procedures should be established for file system design
5. Operation Systems should be configured to timeout and clear the screen automatically
6. Each user should be assigned a home directory and access to these home directories should be restricted
7. Procedures should be established for reporting information security incidents on the operating systems
8. Appropriate login process to Operating System, Application and Database should be established
9. Correct setting of computer clocks should be ensured
10. Procedures should be established for job scheduling
11. Procedures should be established for User Management Controls
12. Procedures should be established for Authentication Management Controls
13. Procedures should be established for Password Controls
14. Procedures should be established for Log Management Controls
15. Procedures should be established for Change Management Controls
16. Procedures should be established for Incident Management Controls

17. Procedures should be established for Capacity Management Controls
18. Procedures should be established for Backup Management Controls



#### 6.4.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Installation of the Operating Systems</b>
	All operating systems must have appropriate licenses and should be installed by the authorised users only.
<b>2.</b>	<b>Hardening of the Operating Systems</b>
	Minimum Baseline Security Standards or hardening standards for all Operating Systems must be defined, implemented and recorded. All installations of the operating systems must be configured as per these procedures.
<b>3.</b>	<b>Access permissions</b>
	<ul style="list-style-type: none"><li>• Access to OS files/directories, OS commands and sensitive utilities must be restricted to only those users who require them to perform their job functions.</li><li>• Access to start-up and configuration files must be restricted to the System Administrator only, to prevent unauthorized modification of these files.</li><li>• All unnecessary services must be disabled files to prevent unauthorized use of these services.</li><li>• Wherever applicable access to various system utilities must be controlled to ensure that the Users do not obtain more information than what they require to perform their job function.</li><li>• Access to backup utilities must be restricted to only those individuals who require executing them.</li></ul>
<b>4.</b>	<b>File System design</b>
	<p>The System Administrator must design the file system keeping the following points in mind:</p> <ul style="list-style-type: none"><li>• Live or production data must be kept in a separate file system</li><li>• Test / Demo applications must be installed and tested on a separate server. Wherever a test / demo server cannot be provided, a separate file system must be created for the test / demo applications.</li><li>• The Systems Administrator must keep a record of the above designed file systems.</li></ul>
<b>5.</b>	<b>Timeout setting</b>
	Wherever technically feasible the Operation Systems should be configured to timeout and clear the screen automatically, if a client terminal / workstation is inactive for more than 5 minutes.

<b>6.</b>	<b>Home directories</b>
	Each user must be assigned a separate personal / home directory. A user must not have access to another user's home directory.
<b>7.</b>	<b>Reporting of incidents</b>
	<ul style="list-style-type: none"> <li>Whenever a system is suspected of being compromised by an unauthorized user, it should be immediately reported to Chief Technology Officer and respective Group Head.</li> <li>Appropriate preventive, detective and corrective measures should be followed by the authorised users and necessary evidences gathered and secured.</li> </ul>
<b>8.</b>	<b>Login setting</b>
	<p>Login process to Operating System should: t</p> <ul style="list-style-type: none"> <li>Display a legal / warning caption, warning the Users that the computer must only be accessed by authorized Users only.</li> <li>Not provide help messages during the login procedure that would aid an unauthorized User.</li> <li>Validate the login information only on completion of all input data. If an error condition arises, the system must not indicate which part of the data is correct or incorrect.</li> </ul>
<b>9.</b>	<b>Clock setting</b>
	<ul style="list-style-type: none"> <li>The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidences.</li> <li>Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, e.g. Universal Coordinated Time (UTC) or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and correct any time variation.</li> </ul>
<b>10.</b>	<b>Job Scheduling</b>
	<p>Privileges for scheduling jobs on the operating systems should be restricted to only those who are authorised.</p> <p>Scheduled jobs should be reviewed at regular intervals.</p>
<b>11.</b>	<b>User Management Controls</b>
	Please refer to the "User and Authorisation Management Procedures"

<b>12.</b>	<b>Authentication Controls</b>
	Please refer to the "Authentication Management Procedures"
<b>13.</b>	<b>Password Controls</b>
	Please refer to the "Password Management Procedures"
<b>14.</b>	<b>Log Management Controls</b>
	Please refer to the "Log Management Procedures"
<b>15.</b>	<b>Change Management Controls</b>
	Please refer to the "Change Management Procedures"
<b>16.</b>	<b>Incident Management Controls</b>
	Please refer to the "Incident Management Procedures"
<b>17.</b>	<b>Capacity Management</b>
	Please refer to the "Capacity Management Procedures"
<b>18.</b>	<b>Backup Management Controls</b>
	Please refer to the "Backup Management Procedures"

#### **6.4.5 Implementation Responsibilities**

- Chief Technology Officer
- System Administrators



## 15. Network Security Policy

### 6.5.1 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

### 6.5.2 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.

### 6.5.3 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
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.
21. Procedures should be established for User Management Controls.
22. Procedures should be established for Authentication Management Controls.
23. Procedures should be established for Password Controls.
24. Procedures should be established for Log Management Controls.
25. Procedures should be established for Change Management Controls.
26. Procedures should be established for Incident Management Controls.
27. Procedures should be established for Capacity Management Controls.
28. Procedures should be established for Backup Management Controls.

#### 6.5.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Assigning Ownership</b>
	Since Networking Assets are shared across all the departments and users, "The Chief Technology Officer" will be the Owner of the Network Assets.
<b>2.</b>	<b>Network Diagram</b>
	<ul style="list-style-type: none"><li>• The IT Head will be primarily responsible for defining the Network Design and maintaining an updated diagram.</li><li>• Periodic reviews must be conducted to ensure that the diagram is updated to reflect the current network architecture.</li></ul>
<b>3.</b>	<b>Adequate Testing</b>
	Each Network Component should be adequately tested before moving into production environment. The test report should be held on record.
<b>4.</b>	<b>Assigning IP to network equipment</b>
	IP assignment to network equipment should be based on the network design.
<b>5.</b>	<b>Segregation in networks</b>
	<ul style="list-style-type: none"><li>• 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.</li><li>• Various types of assets should be identified in different zones / domains and controlled through appropriate IP Addressing schemes.</li></ul>
<b>6.</b>	<b>Redundancy of Network Components</b>
	To ensure business continuity (availability of Network), adequate redundancy should be built into the Network Design.
<b>7.</b>	<b>Default Passwords to be changed</b>
	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.
<b>8.</b>	<b>Network components</b>
	<ul style="list-style-type: none"><li>• 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.</li></ul>

	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>9.</b>	<b>Network routing control</b>
	<ul style="list-style-type: none"> <li>• Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the confidentiality of data.</li> <li>• Routing controls should be based on positive source and destination address checking mechanisms.</li> </ul>
<b>10.</b>	<b>Packet filtering / blocking rules:</b>
	<p>Following rules should be considered for adequate protection of network and the data:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Similarly on the interfaces connected to the external / untrusted networks, block incoming packets that claim to have source IP of any internal (trusted) network.</li> <li>• Drop incoming packets with loop back addresses (127.0.0.0)</li> <li>• If the network does not need IP multicast, then block multicast packets</li> <li>• 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)</li> <li>• Block ICMP echo, redirect and mask request messages from outside as these are frequently used by attackers. .</li> <li>• Block incoming packets that claim to have same destination and source IP.</li> <li>• SNMP should be disabled or enabled with good community strings and Access Control Lists (ACLs).</li> </ul>
<b>11.</b>	<b>Unused Interfaces, services and ports to be disabled</b>
	<ul style="list-style-type: none"> <li>• All unused Interfaces and VTYS should be disabled or shutdown.</li> <li>• All unnecessary services and ports must be commented out / closed in the configuration files to prevent unauthorized use of these services.</li> </ul>



<b>12.</b>	<b>Use of Firewalls, Intrusion Detection and Prevention System</b>
	<ul style="list-style-type: none"> <li>Any third party (outside) connection to or from corporate Network (LAN / WAN) must pass through a Firewall.</li> <li>Even the critical systems on the LAN / WAN should be controlled with a network and host based firewall.</li> <li>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.</li> <li>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.</li> <li>Even the critical systems on the LAN / WAN should be similarly controlled with an IDS and IPS.</li> <li>Usage of next-generation firewalls should be ensured in case separate IDS and IPS systems are not deployed.</li> </ul>
<b>13.</b>	<b>Network monitoring</b>
	<ul style="list-style-type: none"> <li>A suitable Network Management System (NMS) should be implemented.</li> <li>Monitoring / detection activities which are an integral part of network management must be performed on a real-time basis</li> <li>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.</li> </ul>
<b>14.</b>	<b>Network browsing</b>
	<ul style="list-style-type: none"> <li>Users must not access areas on the network for which they do not have permission.</li> <li>Network Administrators, where feasible, should use access control lists on routers to restrict unauthorized users from accessing the routers.</li> <li>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.</li> </ul>

	<ul style="list-style-type: none"> <li>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.</li> </ul>
<b>15.</b>	<b>Access authentication</b>
	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.
<b>16.</b>	<b>Network sniffers</b>
	<p>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.</p> <p>All network components including desktops, laptops, servers, routers, switches, firewalls etc. should undergo hardening process as per the policy.</p>
<b>17.</b>	<b>Third Party access to network</b>
	<ul style="list-style-type: none"> <li>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.</li> <li>Temporary User ID and password must be granted with minimum rights that are required to perform the job.</li> <li>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.</li> </ul>
<b>18.</b>	<b>Remote Access Security</b>
	<ul style="list-style-type: none"> <li>Authentication of remote users should be done using two factor authentications like hardware tokens, or a challenge/response etc.</li> <li>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.</li> <li>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.</li> </ul>

	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>19.</b>	<b>Remote diagnostic and configuration port protection</b>
	Appropriate physical and logical controls should be placed over the diagnostic and configuration ports as non-protection can lead to unauthorised access.
<b>20.</b>	<b>Network connection control</b>
	The capability of users to connect to the network should be restricted, in line with the established policies and requirements of the business applications
<b>21.</b>	<b>Secure Data Transmission over Network</b>
	<p>"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).</p> <p>As a best practice, data sent over public network should be encrypted using Transport Layer Security (TLS) which is preferred over SSL.</p>
<b>22.</b>	<b>Data thru web pages over Internet</b>
	<p>"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)</p>
<b>23.</b>	<b>Disable insecure network services</b>
	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)
<b>24.</b>	<b>User Management Controls</b>
	Please refer to the "User and Authorisation Management Procedures"
<b>25.</b>	<b>Authentication Controls</b>
	Please refer to the "Authentication Management Procedures"
<b>26.</b>	<b>Password Controls</b>
	Please refer to the "Password Management Procedures"

<b>27.</b>	<b>Log Management Controls</b>
	Please refer to the "Log Management Procedures"
<b>28.</b>	<b>Change Management Controls</b>
	Please refer to the "Change Management Procedures"
<b>29.</b>	<b>Incident Management Controls</b>
	Please refer to the "Incident Management Procedures"
<b>30.</b>	<b>Capacity Management</b>
	Please refer to the "Capacity Management Procedures"
<b>31.</b>	<b>Backup Management Controls</b>
	Please refer to the "Backup Management Procedures"

#### **6.5.5 Implementation Responsibilities**

- Chief Technology Officer
- Network Administrators

## **16. Internet Security Policy**

### **6.6.1 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.

### **6.6.2 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.

### **6.6.3 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 internet log monitoring.
5. Procedures should be established for restricting abuse of internet access by users.
6. Procedures should be established for usage of internet data card.
7. Procedures should be established for User Management Controls.
8. Procedures should be established for Authentication Management Controls.
9. Procedures should be established for Log Management Controls.
10. Procedures should be established for Incident Management Controls.

#### 6.6.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Access to Internet</b>
	<p>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:</p> <ul style="list-style-type: none"><li>• The nature of work that requires the User to connect to the Internet.</li><li>• The sites that he / she are authorized to access the Internet.</li></ul>
2.	<b>Control over Internet Access</b>
	<ul style="list-style-type: none"><li>• All Internet activity must pass through Firewall so that access controls and related security mechanisms can be applied.</li><li>• Internet access should be restricted to authorized individuals only.</li><li>• Sites that are not related to business activities should be restricted.</li><li>• Sites providing offensive / indecent content should be blocked at all times.</li><li>• 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.</li></ul>
3.	<b>Control over Downloads</b>
	<ul style="list-style-type: none"><li>• 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.</li></ul>
4.	<b>Restrictions on Users</b>
	<ul style="list-style-type: none"><li>• Users are not allowed to host personal sites using Organisation facilities</li><li>• 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.</li><li>• The ability to connect with a specific web site does not in itself imply that the user is permitted to visit that site.</li><li>• The use or attempt to initiate such activities using Organisation's computing facilities or equipment leading to abusive, unethical or</li></ul>

	<p>"inappropriate" use of the Internet are considered grounds for disciplinary, legal and/or punitive actions, including termination of employment.</p> <ul style="list-style-type: none"> <li>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 other information stored on or passing through the Organisation's Information Technology and Network.</li> </ul> <p>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.</p>
<b>5.</b>	<b>Usage of Internet Data card etc. to connect to internet</b>
	<ul style="list-style-type: none"> <li>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.</li> </ul>
<b>6.</b>	<b>User Management Controls</b>
	Please refer to the "User and Authorisation Management Procedures"
<b>7.</b>	<b>Authentication Controls</b>
	Please refer to the "Authentication Management Procedures"
<b>8.</b>	<b>Log Management Controls</b>
	Please refer to the "Log Management Procedures"
<b>9.</b>	<b>Incident Management Controls</b>
	Please refer to the "Incidence Management Procedures"

#### 6.6.5 Implementation Responsibilities

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

## **17. E-mail Security Policy – applicable only in case of clients' own domain**

### **6.7.1 Policy Objective**

- Implement adequate usage controls to ensure that the email facility provided to the USERS is used only for the official purpose. E.g. content filtering, mail box size restrictions, mass mailing controls, attachment size controls etc.
- Protect the Information Assets from various threats related to the usage of E-mails like viruses, spam mails, leakage of information through e-mails etc.
- E-Mail usage should be logged and monitored.
- To encourage an efficient communication system and to add value to the services offered.
- Implement adequate security controls to ensure that the vulnerabilities associated with email facility are minimized e.g. antivirus etc.

### **6.7.2 Policy Scope**

This policy is applicable to the infrastructure supporting the E-mail services like E-Mail Server, Mail Box server, E-Mail application, etc. and is applicable to all users including the employees, contractors, consultants and temporary users.

### **6.7.3 Policy Statement(s)**

1. Procedures should be established for controlling e-mail access.
2. Users should access only the approved client email software.
3. Users should not abuse e-mail access.
4. Procedures should be established for restricting access to other user's e-mail account.
5. Users should not open e-mails / attachments received from unknown source.
6. All incoming and outgoing mails should be scanned for viruses and content filtering.
7. The Management can inspect email and attachment contents of any user at any time without notice.
8. Auto forwarding of e-mails should be restricted.
9. Sending of critical information through e-mails should be controlled.
10. Mail size and Mailbox size should be restricted.
11. Attachment size of e-mails should be restricted.
12. Every e-mail should contain a standard and approved disclaimer.
13. Every user should adopt standard approved e-mail signature.
14. Procedures should be established for ensuring proper backups of e-mail files.



15. Access to Email from outside of Organisation Network should be controlled.
16. Controls over distribution email Ids should be established.
17. Procedures should be established for securing and maintaining e-mail logs.
18. Procedures should be established for User Management Controls.
19. Procedures should be established for Authentication Management Controls.
20. Procedures should be established for Password Controls.
21. Procedures should be established for Log Management Controls.
22. Procedures should be established for Incident Management Controls.
23. Procedures should be established for Backup Management Controls.

#### 6.7.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Controls over E-Mail Access</b>
	Access to the e-mail facility from the Organisation infrastructure should be given to only those users who have a business need.
<b>2.</b>	<b>Only tested and approved e-mail Software</b>
	The users should be allowed to access their emails using the approved client email software only. E.g. outlook
<b>3.</b>	<b>User Responsibility</b>
	<ul style="list-style-type: none"> <li>Each user should be held accountable for contents of his / her email. Each user must have a distinct and unique e-mail ID to help establish accountability.</li> <li>In case of any unusual activity like chain mails, spam emails, virus emails, etc. the user should report it to the Departmental Head.</li> <li>Each employee should be responsible for the contents of his/her e-mail and all actions performed using his/her email logon credentials.</li> <li>Email should be used only for business purposes. Personal or non-business use of the Systems is not permitted.</li> <li>Users should use only their own E-Mail account and should not allow anyone else to access their account. Users should identify themselves by their real name; pseudonyms that are not readily attributable to actual users should not be allowed. Users should not represent themselves as another user. Each user should take precautions to prevent unauthorized use of the E-Mail account. Forging of header information in E-Mail (including source address, destination address, and timestamps) is not permitted.</li> <li>Users should not provide other unauthorized persons with their E-Mail ID and password.</li> <li>Users should not send confidential or restrictive information via E-mail, unless it is approved. E-mail should not be used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others. If any employee receives offensive E-mail/s, he / she may either communicate with the originator of the offensive E-mails, asking him/her to stop sending such messages, or report such offensive E-mails directly to Information Security Officer.</li> </ul>

	<ul style="list-style-type: none"> <li>• Users should not post network or server configuration information about any devices to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.</li> <li>• Users who cannot access their email for long periods (due to vacation, outstation work, etc.) may use "Out of Office" feature.</li> <li>• Users should not employ a scanned version of a hand-rendered signature to give the impression that the sender signed an E-mail message or other electronic communications, as another person could misuse the signature.</li> <li>• Users should not modify the security parameters within the E-Mail system.</li> <li>• Users should not send unsolicited bulk mail messages. This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious E-Mail, including but not limited to "mail bombing," is prohibited.</li> </ul>
<b>4.</b>	<b>Restriction on use of another user's email ID</b>
	<ul style="list-style-type: none"> <li>• Users accessing the e-mail services must not use or access an e-mail account assigned to another individual to either send or receive messages.</li> <li>• If there is a need to read other user's e-mail (while he /she are away on vacation for instance), then message forwarding and other facilities should be used instead. An approval from appropriate authority should be obtained in case a user's e-mail needs to be read in his / her absence.</li> <li>• At times emails of some persons need to be accessed on an on-going basis by other/s (E.g. Secretary accessing Boss's email or a Project email id accessed by team members), such facility should be used / allowed only for receiving or reading mails and not for sending mails through that ID. Further, such facility should be allowed only after a formal approval from the business head or from the person who's ID is being used.</li> </ul>
<b>5.</b>	<b>Mails from unknown Sources</b>
	Opening of e-mails and attachments from unknown or un-trusted source is STRICTLY PROHIBITED.
<b>6.</b>	<b>Virus and other controls</b>

	All incoming and outgoing mails should be subjected to scanning for viruses and content filtering.				
<b>7.</b>	<b>Right to review e-mail contents</b>				
	<p>E-mail facility used by USERS from the Organisation's Infrastructure is the property of the Organisation. Accordingly, the management can inspect the email and attachment contents at any time and without notice. This information may be monitored, searched, reviewed, disclosed, or intercepted by the management for any legitimate purpose, including but not restricted to the following:</p> <ul style="list-style-type: none"> <li>• To monitor performance,</li> <li>• Ensure compliance with organisation policies,</li> <li>• Prevent misuse of the Systems,</li> <li>• Troubleshoot hardware and software problems,</li> <li>• Comply with legal and regulatory requests for information, and Investigate disclosure of confidential business, proprietary information, or conduct that may be illegal or adversely affect the organisation or its associates.</li> </ul>				
<b>8.</b>	<b>Restrictions on Auto Forwarding of emails</b>				
	No email, automatic or otherwise, should be forwarded to personal or another user official and public email account unless required by business				
<b>9.</b>	<b>Controls over sending critical information through emails</b>				
	Highly critical and confidential information like passwords, etc. should not be sent through normal email facility. Any other confidential documents sent by email should be password protected and the password should be communicated to the recipient in a secure manner.				
<b>10.</b>	<b>Mail Size and Mailbox Restrictions</b>				
	<p>Maximum allowed mail size and inbox is as per the table mentioned bellow. Exception for deviation can be taken as per business requirements.</p> <table border="1"> <tr> <td>Max Mail Size</td><td>20 MB</td></tr> <tr> <td>Default Inbox</td><td>500 MB</td></tr> </table>	Max Mail Size	20 MB	Default Inbox	500 MB
Max Mail Size	20 MB				
Default Inbox	500 MB				
<b>11.</b>	<b>Standard Disclaimer for all emails</b>				
	A standard and approved disclaimer should be appended to every email sent outside of Corporate Network.				
<b>12.</b>	<b>E-mail signature</b>				
	A standard email signature format will be provided by the management and every user should follow the format.				
<b>13.</b>	<b>Backup of Emails</b>				

	<ul style="list-style-type: none"> <li>• The IT Department should ensure that adequate backups of emails on the server are taken.</li> <li>• In case a user needs to backup his / her emails for valid business reasons, the IT department should organise the backup, after obtaining appropriate approval from the requestor's manager.</li> </ul>
<b>14.</b>	<b>Access to Emails from outside</b>
	Access to Emails from outside should be granted only against appropriate approvals from the user's manager.
<b>15.</b>	<b>Controls over distribution email IDs</b>
	<p>Distribution email IDs help in sending mass mails to a section or whole of the organisation. However, such distribution IDs may be abused and hence access to such distribution IDs should be controlled.</p> <ul style="list-style-type: none"> <li>• Mails to such IDs should be allowed to the identified user IDs only</li> <li>• Mailing to such IDs should be allowed only from the corporate network</li> </ul> <p>Any mails received from outside of the corporate domain should be kept in a separate folder for further investigation. The mail should not be forwarded to the member email IDs.</p>
<b>16.</b>	<b>E-mail Logs</b>
	Logs for emails should be secured and maintained for the retention period as required by the regulatory body.
<b>17.</b>	<b>User Management Controls</b>
	Please refer to the "User and Authorisation Management Procedures"
<b>18.</b>	<b>Authentication Controls</b>
	Please refer to the "Authentication Management Procedures"
<b>19.</b>	<b>Password Controls</b>
	Please refer to the "Password Management Procedures"
<b>20.</b>	<b>Log Management Controls</b>
	Please refer to the "Log Management Procedures"
<b>21.</b>	<b>Incident Management Controls</b>
	Please refer to the "Incidence Management Procedures"
<b>22.</b>	<b>Backup Management Controls</b>
	Please refer to the "Backup Management Procedures"

#### 6.7.5 Implementation Responsibilities

- Chief Technology Officer
- E-mail administrators
- The users to whom e-mail access is granted

## **18. Desktop and Laptop Security Policy**

### **6.8.1 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.

### **6.8.2 Policy Scope**

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

### **6.8.3 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.

#### 6.8.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Ownership of desktop / laptop</b>
	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.	<b>Security of desktop / laptop</b>
	All the users must agree to take responsibility for the security of their desktop / laptop and the information it contains.
3.	<b>Software on desktop / laptop</b>
	<ul style="list-style-type: none"><li>• Users must take all reasonable steps to protect against the installation of unlicensed or unauthorized software.</li><li>• Installation and use of unlicensed software (software piracy) is illegal and puts the Organization at significant risk of legal action.</li><li>• Executable software must, whenever possible, be validated and approved by IT Department before being installed.</li><li>• 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.</li><li>• Commercial software (including shareware/freeware) must -<ul style="list-style-type: none"><li>◦ Be approved by respective IT head after getting an approval from CISO for installation on the workstations.</li><li>◦ Have a valid license for each prospective user</li><li>◦ Be checked for all known security risks, including malicious software</li></ul></li><li>• Desktop and laptop users must ensure they comply with data copyright requirements.</li></ul>
4.	<b>Surrender of workstation and other asset</b>
	Upon leaving the employ of, the user must return the workstation and every other asset.

#### 6.8.5 Implementation Responsibilities

- Chief Technology Officer
- IT Support Team



## **19. Security Policy for Handheld/Smart Devices**

### **6.9.1 Policy Objective**

Smartphones/Tablets/Wearable Devices which use Smart Operating Systems such as Android, iOS, Blackberry OS, Windows Phone/Mobile (henceforth referred to as "Smart Devices") are being increasingly used in corporate environments as they provide many of the business required functionalities and convenience. However, these smart devices also present security threats to corporate assets.

This policy is prepared to help ensure confidentiality, integrity and availability of Organisation data.

### **6.9.2 Policy Scope**

This policy is applicable to all users who have access to the Organisation data from their smart devices; Users may include employees, contractors, consultants, partners and third parties.

### **6.9.3 Policy Statements**

1. User Roles and Responsibilities
2. Guidelines for Usage of "Smart Devices"
3. Guidelines for ensuring Security & Access Control
4. Guidelines for Encryption

#### 6.9.4 Detailed Procedures

#	Detailed Procedures
1.	<b>User Roles and Responsibilities – Smart Devices</b>
	<ul style="list-style-type: none"><li>• Users of smart devices should diligently protect such devices from loss/theft and disclosure of company information.</li><li>• The users of smart devices should not change / tamper with the configuration settings done by the IT Department on their devices.</li><li>• In case of loss or compromise of any smart device, the user should immediately inform the IT department.</li><li>• Users are responsible &amp; accountable for each and every action/activity which is performed using their smart device.</li><li>• However, in case of any inadvertent action taken by the user such as, opening/reading an attachment/mail/file from the corporate data resulting in suspicious/unwarranted activity, the IT Department shall investigate the issue further and the user will not be accountable/responsible for that incident.</li></ul>
2.	<b>Guidelines for Usage of “Smart Devices”</b>
	<ul style="list-style-type: none"><li>• Only authorised smart devices shall be allowed to access the corporate network.</li><li>• Whenever necessary and after approval, smart devices of guests may be allowed to access the Guest Wi-Fi Network for connecting their devices to internet only. This network should be isolated from the Corporate network.</li></ul>
3.	<b>Guidelines for ensuring Security &amp; Access Control</b>
	<ul style="list-style-type: none"><li>• IT Department shall control the access to corporate data by implementing adequate authentication and authorisation measures.</li><li>• Secure and robust smart device management solution should be implemented to ensure the security of confidential &amp; sensitive corporate data residing on the smart device.</li><li>• Below features are recommended for the smart device management solution:<ul style="list-style-type: none"><li>○ Detect and block devices which are rooted/jail-broken.</li><li>○ Secure/protect configuration software installed on the device.</li><li>○ Encryption of corporate data.</li><li>○ Partition/Isolation/Sandboxing for corporate data.</li></ul></li></ul>

	<ul style="list-style-type: none"> <li>○ Control &amp; manage access restrictions between personal &amp; corporate data.</li> <li>○ Selective wipe of corporate data/applications.</li> <li>○ "Remote lock the device" and "Remote wipe the device".</li> <li>○ Logging of activities performed by the users using corporate data.</li> <li>○ Mandate &amp; re-enforce the policies. For e.g. password policy.</li> <li>○ Blacklist certain applications &amp; services.</li> <li>○ Block devices performing suspicious/unwarranted activity.</li> </ul>
<b>4.</b>	<b>Guidelines for Encryption</b>
	<ul style="list-style-type: none"> <li>● Corporate data residing on the internal/external/removable storage of smart devices should be encrypted in order to prevent data theft,</li> <li>● Corporate data transmission should be encrypted while the device is at rest or in transit.</li> <li>● Only company authorised third-party encryption software should be used if the native platform does not offer the facility of data encryption.</li> </ul>

#### **6.9.5 Implementation Responsibilities**

- IT Support Team
- Departmental Heads
- All USERS

## **20. Virus Protection Policy**

### **6.10.1 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.

### **6.10.2 Policy Scope**

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

### **6.10.3 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.
10. Procedures should be established for controls over mobile code.

#### 6.10.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Selection of the Anti-Virus Software</b>
	<p>Selection of the Anti-Virus software is a critical decision and should be taken considering the following factors.</p> <p>The AV Software should be able to</p> <ul style="list-style-type: none"><li>• Be deployed from a central AV Server on all the servers, desktops, internet proxies and gateways, E-Mail servers etc.</li><li>• Identify and eradicate all known viruses and their variants</li><li>• Send alerts to the user and administrators about any infections</li><li>• Able to get update releases in a timely manner as per the SLA Terms and Conditions.</li><li>• Scan memory, floppies, removable media, USB drives, local and network drives, BIOS, e-mails and attachments, internet browsing and downloads etc.</li><li>• Should have adequate controls to ensure against modifications except by the authorized AV Administrators.</li></ul>
2.	<b>Vendor support</b>
	<p>The ISC should ensure that an appropriate Service Level Agreement (SLA) is entered into with the AV Vendor covering following clauses</p> <ul style="list-style-type: none"><li>• Intimations about any virus outbreaks.</li><li>• Updates / new signatures should be made available not later than one day.</li><li>• Intimation about the intermediate compensating control measures to be taken before the updates / signatures for a new virus are released.</li><li>• In case of a virus infection in the Corporate network, the vendor should support for eradication.</li></ul>
3.	<b>AV Software to be installed on all servers and workstations</b>
	<p>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.</p>
4.	<b>Controls over the Development and Test environments</b>
	<ul style="list-style-type: none"><li>• The Application Service Provider who is engaged in the development and maintenance must ensure that any patches, fixes, upgrades etc. released are virus free.</li></ul>

	<ul style="list-style-type: none"> <li>• When delivered, these new programs should be tested for functionality as well as checked for viruses.</li> <li>• AV software in the test and development environments must be kept up-to-date with latest signatures.</li> </ul>
<b>5.</b>	<b>AV Software setting</b>
	<p>The AV Software settings should be as under:</p> <ul style="list-style-type: none"> <li>• Invoke automatically at the start up</li> <li>• The AV administrator should protect the AV software settings with a password, so that the users cannot modify them</li> <li>• Automatically scan the floppies, USB drives, incoming mails and attachments, internet browsing and downloads, shares etc.</li> <li>• All types of files to be scanned without any EXCLUSIONS.</li> <li>• Automatic updates should be installed from a central server.</li> <li>• Scheduled for scan the entire hard disk at least once a week.</li> </ul>
<b>6.</b>	<b>AV on mobile computing devices like laptops</b>
	<ul style="list-style-type: none"> <li>• The ISC should set up a process of installing and keeping up-to-date, the AV software on all laptops.</li> <li>•</li> </ul>
<b>7.</b>	<b>Third Party Laptops</b>
	<ul style="list-style-type: none"> <li>• Third parties should not be allowed to connect their laptops to the Corporate Network.</li> <li>• If it is necessary, then the laptop must be scanned for viruses with the approved AV Software before allowing on the network.</li> </ul>
<b>8.</b>	<b>Reporting of Infection</b>
	<p>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.</p>
<b>9.</b>	<b>User Education</b>
	<p>The ISC should ensure that the users are given adequate training on the following</p> <ul style="list-style-type: none"> <li>• Users should use only the approved workstations and software.</li> <li>• Users should ensure that the AV software on their workstation is up-to-date.</li> <li>• Users must not attempt to change the setting of the AV software.</li> <li>• User must not install freeware, downloaded or unapproved software.</li> </ul>

	<ul style="list-style-type: none"><li>• 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.</li></ul>
--	--

#### **6.10.5 Implementation Responsibilities**

- Various departments
- Chief Technology Officer
- IT Team

## **21. Patch Management Policy**

### **6.11.1 Policy Objective**

The objective of this Policy is to ensure that

- Establish adequate controls for security of the operating systems, database and web servers.
- 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.

### **6.11.2 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.

### **6.11.3 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



#### 6.11.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Ensure up to date patches for various systems and devices</b>
	<p>The Administrators should ensure that patches released for various Information Assets like Applications, Web Servers, Databases, Operating Systems, Network Switches/Routers/Firewalls etc.</p> <p>The patch management procedures should include the identification, categorization and prioritization of patches and updates.</p>
<b>2. .</b>	<b>Database Security Patches</b>
	<ul style="list-style-type: none"><li>• 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.</li><li>• It should be ensured that the latest security patches for the databases are applied at the earliest.</li><li>• Normally, patches should be installed taking a scheduled downtime.</li><li>• However, if there is a need to apply emergency patches, such updates may be installed even as an unscheduled activity.</li></ul>
<b>3.</b>	<b>Ensure up to date Webserver Security Patches</b>
	<p>Ensure that the web server is up-to-date with latest patches including the SSL/TLS patches.</p> <p>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.</p>
<b>4.</b>	<b>Ensure up to date patches for Network Devices</b>
	<p>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.</p>

#### 6.11.4 Implementation Responsibilities

- Accountability of updating patches is of respective asset owners.

## **22. User and Authorisation Management Policy – for 2 person staff broker/dp it will not be applicable**

**Keep header – As company does not use / has only two people – no need. As when it is increased – the**

### **4.1.1 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.

### **4.1.2 Policy Scope**

This policy covers all USERS and their authorisations

### **4.1.3 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

#### 4.1.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Establish controls over default users</b>
	<p>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.).</p> <p>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.</p>
2.	<b>User Creation, Modification and Deletion</b>
	<ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• 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.</li><li>• 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</li><li>• Generally it is advisable that a deleted user ID is not PURGED but labelled as "deleted".</li></ul>
3.	<b>Identification of Dormant and Inactive User IDs</b>
	<p>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.</p>
4.	<b>Reissue of a disabled User ID</b>
	<p>A disabled/Inactive user ID may be re-activated if necessary, against approvals and must be enabled only for the "original user".</p>

	<p>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.</p> <p>This activity should be logged and monitored.</p>
<b>5.</b>	<b>Assignment of Roles and Groups</b>
	<p>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.</p> <p>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.</p>
<b>6.</b>	<b>Naming Convention</b>
	<p>For all users on other systems (Database, Operating Systems etc.), a naming convention should be defined.</p> <p>The naming convention should help uniquely identify a user on the system.</p>
<b>7.</b>	<b>Unique Identification of each user on a system</b>
	<p>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.</p>
<b>8.</b>	<b>Generic User Ids</b>
	<p>As a prudent practice, creation and usage of generic user Ids for operations and management of IT should be avoided.</p> <p>However, there are situations where creating unique user IDs itself may result in vulnerability e.g. creating multiple user IDs with root, administrator, sys, system etc. privileges. There are also situations where, generic IDs are required for testing purposes.</p> <p>In such cases, the Custodian of the Information Asset should approve shared usage of such generic user Ids by the identified team members.</p> <p>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 accurately identify the user and establish accountability for activities carried using the shared generic user ID.</p>
<b>9.</b>	<b>Locking of a User after certain number of Failed Login Attempts</b>

	<p>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.</p> <p>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 3<sup>rd</sup> Dec 2018)</p>
<b>10.</b>	<b>Temporary User IDs</b>
	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.
<b>11.</b>	<b>User Inactivity Time Out</b>
	<ul style="list-style-type: none"> <li>• Inactivity time out should be configured at 10 minutes.</li> <li>• The user should be required to enter his / her password to unlock the screen.</li> </ul>
<b>12.</b>	<b>Segregation of Duties</b>
	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.
<b>13.</b>	<b>Maker – Checker Controls (Never Alone Principle)</b>
	<p>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.</p> <p>Similarly, maker – checker controls should also be implemented over the transactions done by general users of the application.</p> <p>As a principle, one user should not be able to complete a transaction / activity end-to-end.</p>
<b>14.</b>	<b>Review of Users and their Privileges</b>
	The CISO should ensure that review of Users and their Privileges is carried out at least once a year.

#### **4.1.5 Implementation Responsibilities**

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

## **23. Password and Authentication Management Policy**

### **4.2.1 Policy Objective – other than the applications provided by the Exchanges**

The objective of this policy is to define and implement password and authentication controls.

### **4.2.2 Policy Scope**

This policy is applicable to all devices and covers all USERS.

### **4.2.3 Policy Statement(s)**

1. Enforce strong Encryption Algorithm
2. Ensure that Default Passwords are deleted or changed.
3. A reasonable minimum Password Length must be enforced
4. System should indicate next password change date
5. Enforce password change after First login to the system
6. Enforce password change after it is RESET by the Admin
7. New Password to be different by certain number of characters
8. The System should ensure that new passwords are used for specified minimum period.
9. Selectively enforce Password Aging
10. Enforce complex composition of Password
11. Passwords not to be shared except for shared system IDs
12. Procedural Password controls should be followed
13. Option to 'Change Password' to be available for the user
14. Systems not to allow certain number of old passwords
15. Critical Passwords to be written down on a standard form
16. Password must be changed upon certain events
17. Appropriate Notice / Warning Banner should be displayed
18. Multi-factor / credential Authentication should be implemented
19. Login Error Message should not be indicative
20. Controls should be implemented on Auto Login features
21. Controls should be established for concurrent Logins
22. Temporal Access Controls should be implemented
23. Controls should be implemented over Session aborted by a user

#### 4.2.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Enforce strong Encryption Algorithm</b>
	<ul style="list-style-type: none"> <li>The algorithm used for encryption should be strong, tested and proven. The encryption algorithm should not be reversible.</li> <li>The encryption algorithm should produce different encrypted values for the same passwords used by different users. While encrypting the algorithm should add SALT. (In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage.)</li> <li>Passwords should be encrypted before being stored in the Application, Database, Operating System, Network systems or any other device.</li> <li>The File / Table / database in which the passwords are stored should be protected with strong access controls</li> </ul> <p>"Passwords, security PINs etc. should never be stored in plain text and should be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances." (SEBI Circular dated 3rd Dec 2018)</p>
<b>2.</b>	<b>Ensure that Default Passwords are deleted or changed</b>
	<p>Some of the systems are installed with vendor defined user IDs and passwords. In some cases these passwords are a public knowledge e.g. password for sys, system, scott for Oracle installation etc. At times the vendor would even hard code the password in the application to facilitate maintenance and could be known to several users of the vendor. These passwords are vulnerable.</p> <p>Hence it must be ensured that the default passwords are changed before moving the system in production environment.</p>
<b>3.</b>	<b>A reasonable minimum Password Length must be enforced</b>
	<p>Password is the first and in most cases the only line of defence and must be enforced in the best possible manner.</p> <p>The System should enforce a minimum 8 character Password.</p> <p>Even SEBI has mandated a reasonable minimum length as under</p> <p>"Any Application offered by Stock Brokers to Customers containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc.</p>



	referred to as "Application" hereafter) over the Internet should be password protected. A reasonable minimum length (and no arbitrary maximum length cap or character class requirements) should be enforced. While it is difficult to quantify password "complexity", longer passphrases have more entropy and offer better security in general. Stock Brokers should attempt to educate Customers of these best practices." (SEBI Circular dated 3 <sup>rd</sup> Dec 2018)
<b>4.</b>	<b>System should indicate next password change date</b>
	Wherever possible, the System should inform the user that his / her password would be due for change by a particular date or after certain number of days. This helps the user to select a good strong password in advance.
<b>5.</b>	<b>Enforce password change after First login to the system</b>
	Wherever possible, The System Administrator should enforce change of password for a new user at his FIRST login to the system.
<b>6.</b>	<b>Enforce password change after it is RESET by the Admin</b>
	Wherever possible, The System Administrator should enforce change of password for a user after it is RESET by the Administrator.
<b>7.</b>	<b>New Password to be different by certain number of characters</b>
	Wherever possible, the System should enforce change of password composition by a minimum of 4 characters i.e. the new password must differ from old by at least 4 characters. This will ensure that the password change is really effective.
<b>8.</b>	<b>New password to be used for a minimum period</b>
	<p>Wherever supported, the System should be configured to disallow a user to change his password for a minimum of 5 days i.e. the user will have to use the new password for a minimum of 5 days before the system will allow him to change. This helps ensure that the change of password is effective.</p> <p>In case the user wants to change the password within those minimum mandatory usage days, he should approach the administrator with a request who will then enable the option to change the password for that user and for that instance only.</p>
<b>9.</b>	<b>Selectively enforce Password Aging</b>
	"Avoid forcing Customers to change passwords at frequent intervals which may result in successive, similar, and enumerated passwords. Instead, focus on strong multi-factor authentication for security and educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication

	<p>reset information (such as e-mail and phone number) are up-to-date.” SEBI Circular dated 3-Dec-2018</p> <p>Although it is a good practice to enforce change of password at periodic intervals, SEBI has indicated that instead of changing passwords at regular intervals, customers should be educated to use strong passwords or passphrases. Further SEBI has indicated that after certain number of days, customers should be requested / reminded to change their password and multi-factor credentials. SEBI has also advised to ensure that the out-of-band authentication reset information such as mobile number and email are up-to-date.</p> <p>Hence for customer facing applications. it is not mandatory to systemically enforce change of passwords / passphrases at regular intervals.</p> <p>For other applications and infrastructure assets like operating systems, web servers, databases etc. the passwords should be changed at regular intervals not later than 90 days.</p>
<b>10.</b>	<b>Enforce complex composition of Password</b>
	<p>Wherever supported and required by the business</p> <ul style="list-style-type: none"> <li>• the Systems should be configured to enforce password with the below character types: <ul style="list-style-type: none"> <li>○ Uppercase characters (A,B,C,D...)</li> <li>○ Lowercase characters (a,b,c,d...)</li> <li>○ Numbers/Digits (0,1,2,3...)</li> <li>○ Special Characters/Symbols (!,@,#,\$...)</li> </ul> </li> <li>• the system should be configured to not allow a user to use any character more than twice.</li> <li>• More than 2 successive characters of numbers should not be allowed in the password e.g. ab, 23, xy etc.</li> </ul>
<b>11.</b>	<b>Passwords not to be shared except for shared system IDs.</b>
	<p>The general USERS should not share their passwords with any other user including the administrator.</p> <p>However this control will not apply to such User IDs which are privileged and shared e.g. sharing of user ID and passwords for root, administrator, etc. This sharing should be limited to a very small number of users.</p> <p>Further, where available the users should use “switch user” like facilities to ensure accountability of the activities</p>

<b>12.</b>	<b>Procedural Password controls should be followed</b>
	<p>Some of the password related controls cannot be enforced systemically. These controls must be followed procedurally as under</p> <ul style="list-style-type: none"> <li>• Passwords should not be embedded in scripts and programs because anyone who has access to the source code would be able to know the passwords.</li> <li>• However, there could be circumstances when the passwords are required to be embedded e.g. the backend password used by the application to access the database and should be treated as EXCEPTIONS at the Policy Level itself.</li> <li>• Also the passwords should not be saved / remembered in the authentication window / prompt, because it can be easily abused.</li> </ul>
<b>13.</b>	<b>Option to 'Change Password' to be available for the user</b>
	Option for change of password should be available to the users without intervention of the Administrator. This will eliminate the dependency of change of password on the administrator.
<b>14.</b>	<b>Systems not to allow certain number of old passwords</b>
	Wherever supported, it should be ensured that the system should not allow the user to select any of his past 5 passwords. The system should be configured to save history of last 5 passwords. The past passwords must be encrypted.
<b>15.</b>	<b>Critical Passwords to be written down on a standard form</b>
	<p>It must be ensured that the critical passwords are available even when the concerned administrator is on leave or not available.</p> <p>This can be ensured by writing down the passwords on a standard paper form and safe keeping it in a secured envelope which should be in custody with the respective department head or Data Centre In-charge.</p>
<b>16.</b>	<b>Password must be changed upon certain events</b>
	<ul style="list-style-type: none"> <li>• All users including administrators should change their passwords in case they suspect that it is compromised.</li> <li>• If the administrator team composition changes, the shared passwords must be changed. E.g. a team member is added or someone leaves.</li> <li>• If the password is used during the absence of administrator by opening the envelop for password.</li> </ul>
<b>17.</b>	<b>Appropriate Notice / Warning Banner should be displayed</b>

	<p>The system should be configured to display a Notice / Warning Banner before the user authenticates himself on the system.</p> <p>Displaying a Notice / warning Banner ensures that users are aware of the consequences of unauthorized access and assists in protection of corporate assets in case of occurrence of an incident.</p>
<b>18.</b>	<b>Multi-factor / credential Authentication should be implemented</b>
	<p>Two credential authentications (User ID and Password) is the most common type of authentication, wherein the password becomes the first and the last line of defence. However, in case of sensitive systems, such an authentication mechanism may not be adequate for user identification because of various weaknesses associated with password as an authentication mechanism e.g. a password can be forgotten, can be a guessable string, can be shared, can be seen by others, could be written down etc. Furthermore in such cases password becomes the only and single line of defence.</p> <p>Hence for sensitive / critical systems a multi-credential authentication may be considered. Apart from the User ID and Password, the other additional authentication mechanisms like token, one time password, Digital Certificates, captcha, biometric, etc. could be considered.</p> <p>Even the SEBI Guidelines have mandated multi factor / credential authentication as under</p> <p>"For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software cryptographic tokens, VPNs, biometric devices, PKI etc.). In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory." (Vide SEBI Circular Dated 3rd Dec 2018)</p> <p>"In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used." (SEBI Circular dated 3<sup>rd</sup> Dec 2018)</p>
<b>19.</b>	<b>Login Error Message should not be indicative</b>
	<p>The Login Error Message should display an appropriately worded message which should not indicate any details about the system. It should not indicate whether the user ID or the Password is incorrect. It should also not indicate privileges of the user ID.</p>
<b>20.</b>	<b>Controls should be implemented on Auto Login features</b>
	<p>Various Auto login facilities are available on the OS, DB, Application etc. However, some of the login facilities introduce vulnerabilities and hence must be controlled. Following are the examples:</p>

	<ol style="list-style-type: none"> <li>1. Trusted Logging in through .rhosts and hosts.equiv on UNIX systems</li> <li>2. Connecting into DB using OS Trusting features / sqldb etc.</li> <li>3. Using Remember Password features in the Application or TOAD.</li> <li>4. Saving passwords in the .netrc files for ftp access</li> <li>5. Embedding the passwords in the scripts / programs</li> </ol>
<b>21.</b>	<b>Controls should be established for concurrent Logins</b>
	<p>Generally any user would need one login at a time. Hence users should not be allowed to login concurrently from multiple work stations. However, there may be situations when concurrent login control cannot be implemented. E.g. there could be generic user Ids which would be used concurrently by a team from multiple workstations. In such cases, the number of concurrent logins to be allowed should be defined and enforced systemically (if possible) or procedurally.</p>
<b>22.</b>	<b>Temporal Access Controls should be implemented</b>
	<p>For additional security on critical devices like Firewall, the Organisation should consider Temporal Access Controls as under:</p> <ol style="list-style-type: none"> <li>1. User may be allowed to login only from the identified location (IP address) for administration of critical devices like e.g. routers, firewalls etc. (Through use of Access Control Lists).</li> <li>2. Day, Date and Time Based Controls - The users may not be allowed to login to the system on a non-working day or public holiday. In addition, a user should not be allowed to login at odd hours of the day.</li> </ol> <p>Since these methods may cause operational difficulties, these controls should be implemented with caution and care.</p>
<b>23.</b>	<b>Controls should be implemented over Session aborted by a user</b>
	<p>In case a user aborts his / her session instead of a clean logout, the application should have following features.</p> <ol style="list-style-type: none"> <li>1. The Application should delete this defunct session after the inactivity time out is reached.</li> </ol> <p>The user should be allowed to immediately login (before the timeout period is reached) to the system which should delete the earlier defunct session.</p>

#### 4.2.5 Implementation Responsibilities

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

## **24. Teleworking Policy**

### **6.13.1 Policy Objective**

To prevent unauthorised access to Information Processing Facilities from untrusted networks

### **6.13.2 Policy Scope**

This policy is applicable to all users who need to work from outside of the office network (over untrusted network).

### **6.13.3 Policy Statement(s)**

1. Teleworking need to be established.
2. Teleworking against approval to only selected users.
3. Ensure Security of data over the Network.
4. Teleworker should be given understanding about Security Requirements.
5. Obtain NDA / undertaking from Teleworker.
6. Right to audit Teleworking equipment and environment.
7. Use only the approved hardware and software.
8. Implement User Management Controls.
9. Implement Authentication Management Controls.
10. Implement Password Management Controls.
11. Implement Log Management Controls.
12. Procedures should be established for Backup Management Controls.

#### 6.13.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Teleworking need to be established</b>
	Teleworking should be allowed to only those users to demonstrate the business requirement
<b>2.</b>	<b>Teleworking against approval to only selected users</b>
	Teleworking should be given to selected users and the requirement should be documented and approved by the business head.
<b>3.</b>	<b>Ensure Security of data over the Network</b>
	Generally teleworking will use public / untrusted network e.g. from home, hotel, airport etc. over a data card or public Wi-Fi or internet café. Appropriate technologies must be used to ensure that the data/information on the network is secured e.g. using token based VPN etc.
<b>4.</b>	<b>Teleworker should be given understanding about Security Requirements</b>
	The teleworker should be given adequate understanding about the security controls that he / she must follow including theft/loss of teleworking facility (e.g. laptop).
<b>5.</b>	<b>Obtain NDA / undertaking from Teleworker</b>
	<p>Obtain an undertaking / NDA from the teleworker about practice of the defined controls over the teleworking equipment (e.g. laptop) and ensure confidentiality of the information. The teleworking equipment must be approved and hardened as necessary.</p> <p>The NDA should cover amongst other the following points</p> <ul style="list-style-type: none"> <li>• The users should be advised to ensure appropriate level of Physical and Environmental Security Controls over the teleworking devices</li> <li>• The users should not be permitted to install any software. Only the authorised administrators should install approved software after obtaining necessary approval.</li> <li>• The users should be advised to ensure that the Anti-Virus is updated at regular intervals and is kept up-to-date.</li> <li>• The users should be advised not to tamper with the Anti-Virus set up on the teleworking devices.</li> </ul>
<b>6.</b>	<b>Right to audit Teleworking equipment and environment</b>
	The Organisation has the right to audit the teleworking equipment as well as the environment used by the teleworker e.g. his home from where he would use the equipment.



<b>7.</b>	<b>Use only the approved hardware and software</b>
	The teleworker must ensure to use only the Organisation supplied hardware and software to do teleworking.
<b>8.</b>	<b>Implement User Management Controls</b>
	Please refer to the "User and Authorisation Management Procedures"
<b>9.</b>	<b>Authentication Controls</b>
	Please refer to the "Authentication Management Procedures"
<b>10.</b>	<b>Password Controls</b>
	Please refer to the "Password Management Procedures"
<b>11.</b>	<b>Log Management Controls</b>
	Please refer to the "Log / Audit Trail Control Procedures"
<b>12.</b>	<b>Backup Management Controls</b>
	Please refer to the "Backup Management Procedures"

#### **6.13.5 Implementation Responsibilities**

- IT Department
- Teleworking User

## **25. Encryption Policy**

### **6.14.1 Policy Objective**

The USERS must ensure that the confidential / restricted data is encrypted while it is in transmission and / or stored on storage media.

### **6.14.2 Policy Scope**

This Policy applies to all USERS and critical data / information.

### **6.14.3 Policy Statement(s)**

1. Identify the data / information to be encrypted.
2. Identify the legal/regulatory/contractual requirements.
3. Identify a strong encryption algorithm.
4. Ensure Security of Data on the Network
5. Ensure use of only the Approved Encryption Technology.
6. Ensure access to only authorised USERS
7. Ensure Secure Encryption Key Management.
8. Maintain Key Escrow
9. Consider use of Digital Signatures.

#### 6.14.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Identify the data / information to be encrypted</b>
	The Business Heads / users will be responsible to identify data / information assets which need to be encrypted.
<b>2.</b>	<b>Identify the legal/regulatory/contractual requirements</b>
	The Business Head / user will identify the legal / regulatory / contractual requirements for encryption and accordingly inform the Company IT Head.
<b>3.</b>	<b>Identify a strong encryption algorithm</b>
	<p>The CTO will identify and approve one / more encryption algorithm/s. The selected algorithm should help ensure compliance with the regulatory / Legal / Contractual requirements. Such algorithm should also be compatible with the technology.</p> <p>At times there may be a requirement of separate encryption algorithm / tool / application for some business vertical, which will be approved by the CTO.</p>
<b>4.</b>	<b>Ensure Security of Data on the Network</b>
	Confidential / restricted information transmitted over any communication network, must be sent in an encrypted form.
<b>5.</b>	<b>Ensure use of only the Approved Encryption Technology</b>
	Only the Approved encryption technology should be used for securing confidential / restricted information.
<b>6.</b>	<b>Ensure access to only authorised USERS</b>
	Access to encryption software must be restricted to the authorized USERS only.
<b>7.</b>	<b>Ensure Secure Encryption Key Management</b>
	<p><b>Composition of Key</b></p> <p>The encryption system must be configured in such a manner that would prevent users from employing keys that do not conform to the Password Management Policy. Wherever possible user Passphrase instead of password.</p>
	<p><b>Life (Maximum) of Encryption Keys</b></p> <p>Encryption keys must be changed at regular intervals.</p> <p>In certain cases where changing of keys at regular intervals may not be practical, an exception should be obtained.</p>

	However, where the key is suspected to have been compromised, the encryption key must be changed immediately and associated procedural controls should be complied.
	<b>Disclosure of Encryption Keys</b> Encryption keys are the most sensitive type of information and access to such keys must be strictly limited to those who have a need-to-know and are specifically approved for the purpose.
	<b>Protection of Encryption Keys</b> Encryption keys must not be transmitted over the network in clear text. If the keys used to govern the encryption process are to be transmitted over the network then they must be transmitted in an encrypted manner. Wherever practical, USERS should adopt 'Key Splitting' so that no single user has full knowledge of the encryption key. The keys should be split into two halves and should be held and used securely by two different individuals.
<b>8.</b>	<b>Maintain Key Escrow</b>
	The keys (both halves) used for encryption must be written down and stored in envelopes as per the guidelines in Password security policy. Knowledge and access of the escrow function must be restricted to authorised persons only.
<b>9.</b>	<b>Consider use of Digital Signatures</b>
	The USERS may consider use of Digital signatures to protect the authenticity, integrity and non-repudiation of important electronic documents and also for financial transactions.

#### 6.14.5 Implementation Responsibilities

- IT Support Team
- Departmental Heads of
- USERS

## **26. Clear Desk Clear Screen Policy – for more than 5 people staff**

### **6.15.1 Policy Objective**

The objective of the policy is to ensure that the Desktops, Laptops, paper and computer media containing confidential information and all associated equipment are stored suitably in a secured manner when not in use to reduce the risk of unauthorized access.

### **6.15.2 Policy Scope**

The policy applies to:

- All the information regardless of whether it is stored electronically or in paper format.
- All users
- All associated devices like computers, terminals, facsimile machines, photocopiers, printers etc.

### **6.15.3 Policy Statements**

1. Ensure that the USERS follow "Clear Desk" Practices.
2. Ensure Security of Personal Items.
3. Ensure security of printouts.
4. Ensure Security of information discussed during meetings.
5. Ensure that USERS follow "Clear Screen" Practices.
6. Ensure Security of Laptop and Smart Devices like Mobile Phones.
7. Procedures should be established for protection of paper and removable media.
8. Procedures should be established to ensure need-to-know.

#### 6.15.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Ensure that the USERS follow "Clear Desk" Practices</b>
	USERS should lock their workstation, laptops and any other confidential assets (paper and magnetic) in cabinets or desk drawers (as appropriate) when the desk is unattended for an extended period - for example when away for meetings, at lunch times, or overnight.
<b>2.</b>	<b>Ensure Security of Personal Items</b>
	Users should ensure that all the personal items (i.e. keys, handbags, wallets etc.) are locked safely. The owners should ensure that necessary security precautions are taken. The users will be responsible for security of their personal belongings.
<b>3.</b>	<b>Ensure Security of Printouts</b>
	Users should ensure that the documents are immediately retrieved from printers and fax machines as soon as possible after printing.
<b>4.</b>	<b>Ensure Security of information discussed during meetings</b>
	On conclusion of meetings where important issues are discussed, the users should ensure that confidential information is not left in the meeting room, either on the table, screens or whiteboards, etc.
<b>5.</b>	<b>Ensure that USERS follow "Clear Screen" Practices</b>
	<ul style="list-style-type: none"> <li>• Users should ensure that computers and laptops are not left logged on when unattended, and are locked with password-protected screensavers.</li> <li>• Users should close / minimize / lock the screen when unauthorised persons are in close proximity to the screen.</li> <li>• The workstation DESKTOP should not be cluttered.</li> </ul>
<b>6.</b>	<b>Ensure Security of Laptop and Smart Devices like Mobile Phones</b>
	<ul style="list-style-type: none"> <li>• If any user has to use his / her laptop in a public place, e.g. on a train, aircraft or bus, he / she should ensure that it would be positioned in such a manner so that the screen cannot be viewed by others.</li> <li>• When leaving a laptop unattended for any extended period, e.g. lunch breaks or overnight, seminars, the users should: <ul style="list-style-type: none"> <li>○ Physically secure it with a cable lock and/or</li> <li>○ Lock it away in a robust cabinet or alternatively lock the door of an individually occupied office.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• In vulnerable situations, e.g. public areas such as airport lounges, hotels and conference centres, the USERS should ensure that the laptop would never be left unattended.</li> </ul>
<b>7.</b>	<b>Protection of paper and removable media</b>
	Users should ensure that any documents or magnetic media, or other removable media such as CDs, DVDs etc. are stored securely.
<b>8.</b>	<b>Need-to-Know</b>
	Users should ensure that knowledge or possession of sensitive information is to be strictly limited to those who have a need to know and appropriate privileges.

#### **6.15.5 Implementation Responsibilities**

- Information Asset Owners
- Information Asset Custodians
- IT Support Team
- USERS

## **27. Capacity Management Policy**

### **6.16.1 Policy Objective**

- To ensure that the technology and other resources are able to scale up to the requirement of growing business volumes.
- To perform appropriate sizing of the infrastructure.

### **6.16.2 Policy Scope**

- Hardware Infrastructure
- Operating Systems
- Application Systems
- Database Systems
- Network Infrastructure
- Data Centre Infrastructure

### **6.16.3 Policy Statement(s)**

1. Responsibility of capacity management should be established
2. Procedures should be established for monitoring capacity utilization
3. Procedures should be established for capacity management



#### 6.16.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Responsibility of capacity management</b>
	<ul style="list-style-type: none"> <li>The IT Department and General Administration Department is responsible for calculating the capacity requirements for various information assets like Hardware Infrastructure, Server Operating Systems, Application Systems, Database Systems, Network devices and Network Infrastructure (Bandwidth and redundancies) and the supporting Data Centre Infrastructure like UPS, Power Generator, Air Conditioners, Fire Extinguishers etc.</li> <li>While calculating capacity of any information asset the CTO should work closely with the Business Heads to understand the present and projected volumes for a reasonable period in future. The business projections will help the CTO to plan capacity of the future procurements.</li> </ul>
2.	<b>Capacity Management</b>
	<b>Data Centre Infrastructure</b> <p>While calculating the capacity of the data centre the present and future business expansion plans should be considered. Following aspects should be considered while deciding on the capacity management of the Data Centre</p> <ul style="list-style-type: none"> <li>Floor Space</li> <li>Power supplies and UPS with Battery backup</li> <li>Air conditioning</li> <li>Fire Extinguishing systems</li> </ul>
	<b>Information Technology Infrastructure</b> <p>While calculating the capacity of the I.T. Infrastructure, the present and future business expansion plans should be considered. Following aspects should be considered while deciding on the capacity I.T. Infrastructure</p> <ul style="list-style-type: none"> <li>Hardware</li> <li>Operating Systems</li> <li>Application Systems</li> <li>Databases</li> <li>Web Servers</li> </ul>
	<b>Network Infrastructure</b> <p>Similarly while calculating the capacity of the Network Infrastructure the present and future business expansion plans should be considered. Following aspects should be considered while deciding on the capacity management of the Networking Infrastructure</p> <ul style="list-style-type: none"> <li>Network Architecture</li> </ul>

	<ul style="list-style-type: none"> <li>• Bandwidth Requirements</li> <li>• Backup / fall back lines</li> <li>• Network Monitoring Systems</li> <li>• Firewall and IDS – IPS requirements</li> </ul>
<b>3.</b>	<b>Monitoring Capacity Utilisation</b>
	<p>It is necessary that the installed capacity should be continuously monitored by the IT Department, to ensure its adequacy to meet the user and / or business requirements and cyber resilience. Threshold limits should be established for various information assets and utilisation should be monitored against these threshold limits. Wherever possible, automated alerts should be sent out to the designated users whenever the utilisation exceeds the threshold limits.</p> <p>Following aspects should be considered for monitoring capacity utilisation</p> <ul style="list-style-type: none"> <li>• Network bandwidth utilisation</li> <li>• Asset Performance</li> <li>• Memory utilisation</li> <li>• Disk and Storage Utilisation</li> <li>• Utilisation of Critical systems and networks which are exposed to the Internet</li> </ul>

#### **6.16.5 Implementation Responsibilities**

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

## 28. Change Management Policy

### 7.1.1 Policy Objective

The Change Management Policy is designed to

- Ensure that each change is documented, studied for feasibility, approved and tracked till movement into production environment.
- Each change is tested before moving into production environment.
- The user and technical documentation is updated for the respective system.
- Provide for a mechanism for urgent changes to be carried in exceptional circumstances.
- Roll back of the change is provided.

### 7.1.2 Policy Scope

This policy is applicable to changes pertaining to Application systems and supporting Infrastructure.

### 7.1.3 Policy Statement(s)

1. Changes to software must be controlled
2. Each Change Request with reasoning, module, problem expected to be resolved etc. must be recorded even if not considered for change.
3. Each change request should be studied for its' feasibility.
4. Criticality, priority and scale of change should be studied.
5. Emergency changes should be handled appropriately
6. The target date of change requirement should be decided.
7. Procedures should be established for testing by developer.
8. Procedures should be established for risk and impact analysis.
9. Procedures should be established for user acceptance testing.
10. Procedures should be established for migration of changes to production environment.
11. Procedures should be established for replication of successful changes.
12. Procedures should be established for carrying out necessary changes to documentation.
13. Procedures should be established for closure of change requests.

#### 7.1.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Changes to software must be controlled</b>
	Generally changes / modifications to the software package / application should be discouraged, unless it is required to address / improve the business functionality. Further changes to the software packages should be limited / restricted to the essential ones only.
2.	<b>Each Request Must be recorded with reasons</b>
	Each Change Request must be recorded with reasoning, module name, problem expected to be resolved etc. This should be practiced irrespective of whether a change request is accepted or rejected. Various other details like the date of request, name of the requester and a running serial number should be given to each request received and tracked till it is closed by movement into production environment or discarded.
3.	<b>Changes must be studied for feasibility</b>
	Each change request should be studied for various aspects like business feasibility, technical feasibility, process feasibility, financial feasibility, legal feasibility and overall impact etc. There may be simple work around available which may produce desired results and the change may not be warranted at all.
4.	<b>Criticality, priority and scale of change should be studied</b>
	Priority, Criticality and scale/category of change should be captured in the change management process along with approval indicating an expected date for closure. On a broad level, the categorisation of changes shall be as follows: <ul style="list-style-type: none"><li>• Minor Changes – Any routine change such as firewall policy changes, enabling/disabling services/features on servers, changing sequence of menus in the Application etc. that has minimal / NO impact.</li><li>• Major Changes – Any routine or non-routine change such as OS/Application/Database upgrade, Firmware upgrade of network devices, Fundamental change in the application i.e. adding or removing modules, correction in the functionality of the application etc. that may have significant impact on users.</li></ul>
5.	<b>Emergency changes should be handled appropriately</b>
	At times, changes are required to be carried out on an urgent basis for ensuring normal business operations.

	Such changes can be performed on a verbal / mail approval from respective authority. Any such change shall be logged and recorded via the regular change management procedure after completion / closure.
<b>6.</b>	<b>Decide the target date of change requirement</b>
	The approved request should be given to the vendor / development team indicating the date by which the change is required. The vendor / development team should accept the target date for completion.
<b>7.</b>	<b>Testing by the developer</b>
	The vendor / development team should complete the development and carry out tests before handing over the new code for User Acceptance Testing.
<b>8.</b>	<b>User Acceptance Testing</b>
	User Acceptance Testing should be carried out in a separate Test Environment before moving the changes to production environment. If rejected, reasons should be documented and given back to the vendor / development team.
<b>9.</b>	<b>Migration to Production</b>
	Precautions against malicious codes should be taken during transition from UAT environment to production environment. Only the finally tested and controlled copy should be migrated to production. After completion of migration, ensure that the access given to developer team is withdrawn.
<b>10.</b>	<b>Replication</b>
	After a change has been successfully implemented in the production environment, it should be replicated to disaster recovery.
<b>11.</b>	<b>Changes to the Documentation and training to users</b>
	It should be ensured that documentation related to the change request is completed. Similarly the system manuals / documentation should be suitably modified.  The affected users should be informed about the changes and if necessary suitable training should be given.
<b>12.</b>	<b>Closure and record</b>
	The Change Request should be closed and record updated.

### 7.1.5 Implementation Responsibilities

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

## **29. Physical and Environmental Security Policy – for Type I broker create a para**

### **2.1.1 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.

### **2.1.2 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.

### **2.1.3 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

#### 2.1.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Implement Physical Access restrictions</b>
	<ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• Access to critical computing facilities should be granted only those who are authorised.</li><li>• USERS / visitors must not attempt to enter restricted areas in the company premises for which they have not been granted access.</li><li>• The access list authorised users should be reviewed at least once a year.</li></ul>
2.	<b>Securing critical equipment / areas</b>
	<ul style="list-style-type: none"><li>• All critical servers and communication equipment must be located in secured rooms to prevent tampering and unauthorized access.</li><li>• 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.</li><li>• 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 and cleaning crew must be supervised at all times whenever they are in the server room / data centre / computing facility.</li></ul>
3.	<b>Logs / Audit Trails should be enabled and reviewed regularly</b>
	<ul style="list-style-type: none"><li>• 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.</li></ul>



	<ul style="list-style-type: none"> <li>If Manual paper based registers are maintained, such registers also should be authorised and reviewed at regular intervals.</li> </ul>
<b>4.</b>	<b>USERS should wear Identification Badges</b>
	Each USER must wear an identification badge to gain access to the premises. The badge must have a photo of the USER
<b>5.</b>	<b>Consider Security Guards where necessary</b>
	<p>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.</p> <p>The security guards are expected to perform following</p> <ul style="list-style-type: none"> <li>Any material coming in or going out is backed up by appropriate challan. These tasks are performed by administration department.</li> <li>Any material sent out which is returnable is appropriately recorded for return on the due date by administration department.</li> <li>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.</li> </ul>
<b>6.</b>	<b>Entry for visitors</b>
	<ul style="list-style-type: none"> <li>Ensure that each visitor entering the secure area makes an entry in Visitor's Book.</li> <li>Ensure that the authorised user escorts the visitors.</li> <li>Visitors Log Register should be reviewed by the Administration dept.</li> </ul>
<b>7.</b>	<b>Implement Controls over Lost Identity Badges</b>
	<ul style="list-style-type: none"> <li>The security officer on intimation of lost / stolen identification badges should immediately deactivate the badge.</li> <li>Identification badges that have been lost or stolen or are suspected of being lost or stolen must be reported to the Admin Department immediately.</li> <li>Process for issuing duplicate identity badges should be started by admin department after receiving required authorisation.</li> </ul>
<b>8.</b>	<b>Prohibit Piggybacking</b>
	<ul style="list-style-type: none"> <li>USERS must not permit unknown or unauthorized persons to pass through doors requiring swipe cards / number codes.</li> </ul>
<b>9.</b>	<b>Choose secure location for the Critical Secure Areas</b>
	<ul style="list-style-type: none"> <li>The Critical Secure Areas should be located in buildings which are adequately strong.</li> </ul>

	<ul style="list-style-type: none"> <li>• 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..</li> <li>• 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.</li> <li>• Likewise, to minimize potential water damage, rest room facilities or water tanks should not be located directly above these facilities.</li> </ul>
<b>10.</b>	<b>Ensure security of Cables / Electrical fittings</b>
	<ul style="list-style-type: none"> <li>• Data Cables connecting computing equipment and other support equipment must be neatly organized (structured cabling). Cabling maps should be prepared.</li> <li>• All electrical wiring and LAN cabling must be structured and run through concealed cabling.</li> <li>• Electrical wiring and LAN cabling MAPs should be prepared.</li> <li>• Circuit breakers of appropriate capacity must be installed to protect the hardware against power surges.</li> <li>• Electrical mains must be properly guarded against accidental / unauthorized access.</li> <li>• Emergency power off switches should be located near the EXIT door to facilitate rapid power down</li> </ul>
<b>11.</b>	<b>Ensure Fire detection and suppression systems are operational</b>
	<ul style="list-style-type: none"> <li>• Smoking should be prohibited within the office premises and critical secure areas.</li> <li>• Smoke detectors must be placed at strategic locations to set off an alarm in case of smoke / fire.</li> <li>• 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.</li> <li>• Smoke detectors must be placed below the raised floor and above the false ceiling of the server room / data centre.</li> <li>• The fire alarm, smoke detectors and extinguisher system must be inspected and tested as per vendor recommendations and at least once a year.</li> </ul>

	<ul style="list-style-type: none"> <li>• Training should be given to the USERS on the use of the fire extinguisher system at least once a year.</li> </ul>
<b>12.</b>	<b>Implement Control against water damage</b>
	<ul style="list-style-type: none"> <li>• Locations of "Secure Areas" with potential for water damage must be avoided.</li> <li>• There must be a master switch / valve for all water mains.</li> <li>• Humidity monitors should be installed in the server room / data centre to control the humidity content.</li> </ul>
<b>13.</b>	<b>Ensure cleanliness of premises and Secure Areas</b>
	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Eating &amp; drinking must be prohibited in the data centre</li> <li>• Users must ensure that their desks are clean (no confidential information should be kept in the open)</li> </ul>
<b>14.</b>	<b>Handling power outages</b>
	<ul style="list-style-type: none"> <li>• 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.</li> <li>• In areas susceptible to outages of power for longer durations, generators should be provided to ensure working of servers and all business critical workstations.</li> <li>• Backup power facilities must be tested at least once a month to ensure reliable functioning of the equipment.</li> <li>• Emergency lighting may be provided for use during power outages.</li> </ul>
<b>15.</b>	<b>Physical access to supporting infrastructure should be controlled</b>
	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.
<b>16.</b>	<b>Implement controls over movement of equipment</b>
	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Appropriate passes/authorization should be issued to effect the removal of equipment from the building.</li> </ul>

<b>17.</b>	<b>Ensure inventory and labelling of all devices</b>
	<ul style="list-style-type: none"> <li>• A complete and up-to-date inventory of all devices should be maintained.</li> <li>• Each Device should be identified with the asset code for easy identification.</li> <li>• Workstations / Laptops must be traceable to individual users. Each individual must be made accountable for the physical security of Workstations / laptop.</li> <li>• When an incident of theft of a Workstations / laptop comes to light it must be reported by the user to the Department Head, &amp; Head-IT and physical security department immediately.</li> </ul>
<b>18.</b>	<b>Ensure Maintenance of equipment</b>
	<p>Equipment should be maintained to ensure its continued availability and integrity. Following guidelines should be considered</p> <ul style="list-style-type: none"> <li>• Equipment should be inspected and maintained in accordance with the suppliers recommended service intervals and specifications.</li> <li>• Only authorized maintenance personnel should carry out repairs and service maintenance.</li> <li>• Appropriate controls should be taken when sending equipment off premises for maintenance. For critical devices transit insurance cover may be obtained.</li> <li>• Only authorised users should be allowed to take the equipment off premises</li> <li>• Appropriate record of movement of such equipment should be maintained for tracking purposes</li> </ul>

### **2.1.5 Implementation Responsibilities**

- Physical Security Department
- Administration Department
- IT Infrastructure Department

## **30. Log / Audit Trail Management Policy – applicable for more than 1 back office users**

### **9.1.1 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 against unauthorized 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.

### **9.1.2 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.

### **9.1.3 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.

#### 9.1.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Define Log Management Strategy</b>
	<ul style="list-style-type: none"> <li>• A Log / audit trail strategy should be designed, documented and implemented to help ensure that the logs are enabled, stored securely, analysed and monitored.</li> <li>• Audit Trails / Logs should be enabled on the Applications and supporting Infrastructure components like Databases, Operating Systems, Web Servers, Switches, Routers and Firewalls.</li> <li>• In case, logging degrades the performance of systems beyond acceptable limits, only selective logging and monitoring of critical commands/ activities may be configured.</li> <li>• 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.</li> </ul>
<b>2.</b>	<b>Ensure that Logs capture only the necessary details.</b>
	The logs should capture details like user Id, Location, activity and date and time to establish accountability.
<b>3.</b>	<b>Logs should not capture sensitive information</b>
	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.
<b>4.</b>	<b>Ensure adequate disk space for saving logs</b>
	To ensure that logging is not disrupted, adequate disk space should be maintained all the time on respective systems.
<b>5.</b>	<b>Ensure Accurate Network Date/Time Stamping</b>
	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.
<b>6.</b>	<b>Ensure Strict Access Controls over Log Files</b>
	The Log files should be access controlled to ensure against unauthorized modifications. Wherever possible, the logs should be enabled in Binary mode.
<b>7.</b>	<b>Enable Logs in Append Mode</b>
	Generally and wherever technically possible, Logs should be enabled in append mode, to ensure that the earlier logs are not overwritten.
<b>8.</b>	<b>Preserve logs as per Retention Period Requirements</b>

	<p>Logs should be saved / retained for a period as required by the applicable regulatory body guidelines.</p> <p>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).</p>
<b>9.</b>	<b>Logs should be analysed as necessary</b>
	<ul style="list-style-type: none"> <li>• Logs help analyse and monitor the system performance, errors, security events, switching of users, login-logout, access failure, user activities, backup activities etc.</li> <li>• Logs generated by various Information Assets like Applications and supporting Infrastructure should be reviewed and analysed at regular intervals.</li> </ul>
<b>10.</b>	<b>Retain logs until completion of investigation</b>
	In case of investigations, the log files should be preserved for the required period of investigation.
<b>11.</b>	<b>Log Host should be defined</b>
	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.
<b>12.</b>	<b>System Installation Logs should be backed up and then removed</b>
	Installation logs should be backed up and then removed from the system, since they may contain installation user ID and passwords.

#### 9.1.5 Implementation Responsibilities

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

## **31. Incident Management Policy for type I & II broker make a small para**

### **8.1.1 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.

### **8.1.2 Policy Scope**

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

### **8.1.3 Policy Statement(s)**

1. Identify the Incident Response Team (IRT).
2. Identify possible Incidents and steps for recovery.
3. Training for Incident Identification
4. Ensure Incident / Problem Reporting
5. Analyse the Incident / Problem
6. Activation of the Incident Response team
7. Contain the Incident / Problem and remove the cause
8. Escalation Process should be established.
9. Root Cause and Impact Analysis should be done
10. Evidence should be collected
11. Implement additional / change of controls



#### 8.1.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Identify the Incident Response Team (IRT)</b>
	<p>An Incident Response Team (IRT) should be identified. The IRT should comprise of the administrators of Application / OS / DB / Network. The Incident Response Team leader should be identified and should be vested with the power to declare and activate the Incident Response Team.</p> <p>Roles and responsibilities of the staff involved in the IRT, including recording, analysing, remediating and monitoring incidents or problems should be clearly defined.</p>
<b>2.</b>	<b>Identify possible Incidents and steps for recovery</b>
	<p>The IRT should ensure that various possible incidents or problems are studied and documented including the steps for resolution.</p> <p>Each possible incident or problem along with the steps should be documented and reviewed and rehearsed at regular intervals.</p> <p>The document should be available with the IRT.</p>
<b>3.</b>	<b>Training for Incident Identification</b>
	<p>Adequate and repeated training should be given to USERS to help them understand and identify an event / incident / problem.</p> <p>This would include demonstration of sirens, alarms, incorrect system behaviour, other indications etc.</p>
<b>4.</b>	<b>Ensure Incident / Problem Reporting</b>
	<p>The users should be informed about the process of incident / problem reporting, to the appropriate authority for an early resolution.</p> <p>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.</p>
<b>5.</b>	<b>Analyse the Incident / Problem</b>
	<p>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.</p> <p>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.</p>
<b>6.</b>	<b>Activation of the Incident Response team</b>

	In case of an incident / problem, the head of Incident Response Team should declare the incident / problem and activate the response team in a timely manner.
<b>7.</b>	<b>Contain the Incident / Problem and remove the cause</b>
	<p>The Incident Response Team should first try to contain the Incident / Problem to ensure that the damages are minimal.</p> <p>After containment the Incident Response Team should remove the cause of the Incident / Problem.</p> <p>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.</p>
<b>8.</b>	<b>Escalation Process should be established</b>
	<p>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.</p> <p>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.</p> <p>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.</p> <p>In case of breach of regulatory requirements, legal and compliance team will take necessary action to report such incident / breach to the concerned authority.</p>
<b>9.</b>	<b>Root Cause and Impact Analysis should be done</b>
	<p>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.</p> <p>Root Cause Analysis should cover the following:</p> <ol style="list-style-type: none"> <li>a. Root Cause Analysis <ol style="list-style-type: none"> <li>i. When did it happen?</li> <li>ii. Where did it happen?</li> <li>iii. Why and how did the incident / problem happen?</li> </ol> </li> </ol>

	<p>iv. How often had a similar incident / problem occurred over the last 3 years?</p> <p>v. What lessons were learnt from this incident / problem?</p> <p>b. Impact Analysis</p> <p>i. Extent, duration or scope of the incident / problem including information on the systems, resources, customers that were affected;</p> <p>ii. Magnitude of the incident / problem including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; and</p> <p>iii. Breach of regulatory requirements and conditions, if any, as a result of the incident / problem.</p> <p>c. Correction and Corrective Measures</p> <p>i. Immediate correction to be taken to address consequences of the incident / problem. Priority should be placed on addressing customers' concerns and / or compensation;</p> <p>ii. Measures to address the root cause of the incident / problem; and</p> <p>iii. Measures to prevent similar or related incidents / problems from occurring.</p> <p>The root cause analysis will help identify the control weaknesses in technology and processes.</p>
<b>10.</b>	<b>Evidence should be collected</b>
	<p>Collecting and preserving evidence and documenting the particulars of an incident / problem is essential for meeting a range of reporting requirements and gathering evidence that may be used in legal proceedings.</p> <p>Evidence should be collected as soon as it is reasonably possible and be preserved, documented, and/or tracked by:</p> <ul style="list-style-type: none"> <li>• Ensuring that the scene of the incident / problem is secured and preserved</li> <li>• Collecting physical evidence and observing a strict chain of custody protocol</li> <li>• Conducting interviews</li> <li>• Collecting any other documentation relevant to the incident</li> </ul>
<b>11.</b>	<b>Implement additional / change of controls</b>

	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.
--	---

#### **8.1.5 Implementation Responsibilities**

- The Incident Response Team
- The IRT Leader
- Administrators of various systems – Operating Systems, Application, Database, Routers, Firewalls etc.
- IT Support Team

## **32. Backup Management Policy – Type zero and I – convert it to two small para**

### **10.1.1 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.

### **10.1.2 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.

### **10.1.3 Policy Statement(s)**

1. Asset owner should define the backup requirements.
2. Decide if backup needs to be encrypted.
3. Update the backup requirements as required.
4. Obtain Vendor support as necessary.
5. Assign Backup responsibility.
6. Review of Backup Plan.
7. Maintain Documentation and Records of Backups.
8. Maintain Inventory of Backup Media
9. Backup Media should be appropriately labelled.
10. Ensure Rotation/recycling of backup media
11. Store Backup Media as per vendor recommendations.
12. Store Backup Media in a safe and secure location
13. Controls over movement of Tapes.
14. Backup Media should be tested regularly
15. Controls over retirement of Backup Media.

16. Establish Controls for physical destruction of retired media.

#### 10.1.4 Detailed Procedures

#	Detailed Procedures
1.	<b>Asset owner should define the backup requirements</b>
	<ul style="list-style-type: none"><li>• 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.</li><li>• The information asset owners will decide appropriate backup plan, taking into consideration its importance to the business, legal requirements and technology available.</li></ul> <p>The backup requirements shall be defined using below mentioned guidelines:</p> <ul style="list-style-type: none"><li>• Name and contact details of the owner of the asset</li><li>• Name and contact details of the custodian OR coordinator (appointed by the owner) of the asset for all backup related activities</li><li>• New requirement / change in existing backup requirement</li><li>• The details of servers / drives / folders / files to be backed up</li><li>• The frequency of backups (daily, weekly etc.)</li><li>• Whether local backup required (on a separate Hard Disk/Tape)</li><li>• The type of backup (incremental / differential / full backup etc.)</li><li>• Number of sets – One or Two</li><li>• Whether storage at off site is required</li><li>• State of the Database to be backed up (Cold, Hot, Export, etc.)</li><li>• The retention period</li><li>• Whether data needs to be encrypted or not</li></ul>
2.	<b>Decide if backup needs to be encrypted</b>
	<p>The information asset owners should decide whether the backup needs encryption, type of encryption, etc. taking into consideration its importance to the business, legal requirements, feasibility and available technology.</p>
3.	<b>Update the backup requirements as required</b>
	<p>Every change/modification should be intimated immediately for which the same procedures would be followed as stated above. The change or modification related to backup will be treated as new backup request. All such changes to the backup plan should be approved/ authorized.</p>
4.	<b>Obtain Vendor support as necessary</b>

	Wherever necessary the IT department should organize required support from the Application and Database Vendor/s, to set up the backup for an assured recovery.
<b>5.</b>	<b>Assign Backup responsibility</b>
	<ul style="list-style-type: none"> <li>The Backup Team should ensure that the backups are performed as per approvals received from various business heads.</li> </ul>
<b>6.</b>	<b>Review of Backup Plan</b>
	The backup team head should intimate the respective department heads about the current Backup Plan, which will be reviewed by the Business head who may put forth changes that may be required including addition, modification or discontinuation of the backups. The backup Plan should be reviewed at least once every year.
<b>7.</b>	<b>Maintain Documentation and Records of Backups</b>
	<ul style="list-style-type: none"> <li>The backup plan with schedule should be documented and should be available for reference and verification with the information asset owner and the team responsible for the execution of the backup schedule.</li> <li>The backup plan should also identify the reporting procedures for the execution of the backup schedule and problems encountered.</li> <li>Wherever possible automated logs should be generated for the backup activity and exceptions should be reported to the information owner.</li> <li>The logs of backup activity (either automated or manual) should contain details like <ol style="list-style-type: none"> <li>1. Date and Time of Backup</li> <li>2. Operator name</li> <li>3. Directories and files backed up</li> <li>4. Success or failure – Failures in backups are exceptions and must be reported to the information owner giving brief description of the problem and the status of correction</li> <li>5. Type of backup,</li> <li>6. Backup media type and number,</li> <li>7. Number of writes for that media,</li> <li>8. Retention period etc.</li> </ol> </li> </ul>
<b>8.</b>	<b>Maintain Inventory of Backup Media</b>



	<ul style="list-style-type: none"> <li>Media supplied by vendor should be as per the requisition. The media should be in sealed packed condition before it is accepted.</li> <li>Whenever there is in need of backup media, IT Department will take the approval from CTO and procure the media. It is necessary to update the records in the inventory.</li> <li>A complete inventory should be maintained of <ul style="list-style-type: none"> <li>The media used for backups</li> <li>Unused media (blank),</li> <li>Cleaning Tape Media</li> <li>Media identified for destruction</li> </ul> </li> </ul>
<b>9.</b>	<b>Backup Media should be appropriately labelled</b>
	Each backup taken should be labelled in a manner that will help identify the correct media for restoration without ambiguity. A standard policy for labelling the backed-up media should be followed.
<b>10.</b>	<b>Ensure Rotation/recycling of backup media</b>
	<ul style="list-style-type: none"> <li>Backup media should be rotated ensuring that <ul style="list-style-type: none"> <li>Adequate numbers of generations of backups are available.</li> <li>That no media is reused for taking backups beyond the 'number of writes' as prescribed by the vendor of the media.</li> </ul> </li> </ul>
<b>11.</b>	<b>Store Backup Media as per vendor recommendations</b>
	Backup tapes should be stored in a cool and dust free environment as per the specifications of the Backup Media Vendor.
<b>12.</b>	<b>Store Backup Media in a safe and secure location</b>
	As a best practice, The Backed up Media should be stored in Fire Resistant cabinets.
<b>13.</b>	<b>Controls over movement of Tapes</b>
	<ul style="list-style-type: none"> <li>Backup media should be transported in waterproof and tamper proof Metallic box, having locking facility</li> <li>Movement of media to and from the off site location must be recorded in such a manner that each media is traceable</li> <li>Movement of media should be authorized</li> <li>Movement of media should be done only by the identified person or through the identified agency</li> <li>Keys of the metallic box containing the backed up media, must not be given to the carrier.</li> </ul>
<b>14.</b>	<b>Backup Media should be tested regularly</b>

	<ul style="list-style-type: none"> <li>Backed should be tested for its readability and restorability at regular intervals. The intervals for such testing should be as per the backup plans prepared by the information owner.</li> </ul> <p>The Backup media should be tested at regular intervals to ensure readability and restorability.</p> <ul style="list-style-type: none"> <li>Restoration should be done only in a test environment.</li> <li>Restoration should be possible with the original (as in production) set of directory and file permissions</li> <li>The Asset Owner should verify the test results.</li> <li>If any problems are encountered during test restoration, then the backup plan / procedures should be suitably modified.</li> <li>After the test restoration / recovery is complete, the restored data should be removed</li> </ul>
<b>15.</b>	<b>Controls over retirement of Backup Media</b>
	<ul style="list-style-type: none"> <li>It is very important to discard the media from the backup cycle after vendor recommended read/write operations have been reached. The following procedure is followed to reject / discard any media from the cycle: <ul style="list-style-type: none"> <li>Physically damaged Media</li> <li>Any error occurred while read / write operation on Media. Faulty media are discarded immediately after it is authorized by CTO.</li> <li>Vendor recommended read/write operations have been reached</li> </ul> </li> </ul>
<b>16.</b>	<b>Establish Controls for physical destruction of retired media.</b>
	<p>After confirming that the media has really gone bad or really needs to be destroyed</p> <ul style="list-style-type: none"> <li>After making a record of the media label details and updating the media inventory record which is authorized by the Backup Team Head.</li> <li>Thereafter, the media should be cut into pieces, preferably using special shredders for the purpose.</li> </ul>

#### 10.1.5 Implementation Responsibilities

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

## **33. Business Continuity Management Policy – I & zero – ¾ small para**

### **10.2.1 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.

### **10.2.2 Policy Scope**

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

### **10.2.3 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. Classify the Processes & Supporting Assets.
5. Define Recovery Time & Recovery Architecture for each asset.
6. Implement the BCP.
7. Perform regular Testing of the BCP.
8. Maintain the BCP up-to-date.
9. Maintain and update contact numbers of BC team members.
10. Keep supporting documents updated.
11. Ensure Security of the BC Plan.
12. Audit the BC Plan.

#### 10.2.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Identify the Business Continuity Team leader</b>
	<ul style="list-style-type: none"> <li>• The Business Continuity Team should be headed by the Managing Director or the Owner of the Business Continuity Plan.</li> <li>• The Owner should nominate an alternate team leader to take ownership of the BCP, in his absence.</li> <li>• The Owner should be vested with the power of declaring a disaster.</li> <li>• The Owner should be the executive owner of BC Plan and should be the BC Team leader. The Owner should be responsible for <ul style="list-style-type: none"> <li>○ Identifying the team members for BCP</li> <li>○ Developing and implementing the BCP</li> <li>○ Declaring a disaster and activating the BCP team</li> <li>○ Minimizing the impact of the incident / disaster event and recovering the identified critical assets as per the Business Continuity Plan</li> <li>○ Training the team members</li> <li>○ Testing and keeping the BCP up-to-date</li> </ul> </li> </ul>
<b>2.</b>	<b>Decide the composition of Business Continuity Team</b>
	<ul style="list-style-type: none"> <li>• 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".</li> </ul>
<b>3.</b>	<b>Prepare Inventory of Processes and associated assets</b>
	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.
<b>4.</b>	<b>Classify the Processes &amp; Supporting Assets</b>
	Based on the Risk Management methodology, the owner should classify the criticality of the business process and the associated information assets as per the Risk Management Methodology
<b>5.</b>	<b>Define Recovery Time &amp; Recovery Architecture for each asset</b>
	<ul style="list-style-type: none"> <li>• The asset owners should define the Recovery Time Objective for the assets to define appropriate recovery architecture for the assets. The asset owners should ensure that appropriate Recovery Architecture is defined, so that the assets can be recovered within the Recovery Time Objective. The asset owners should ensure that the recovery architecture and backup requirements are implemented as defined.</li> </ul>

	<ul style="list-style-type: none"> <li>• The asset owners should also define the sequence and priority for recovery from the disaster.</li> <li>• The recovery architecture should also define the process to restore the assets to their normal production environment.</li> </ul>
<b>6.</b>	<b>Implement the BCP</b>
	<ul style="list-style-type: none"> <li>• The selected team members should be trained in their roles and responsibilities as defined within the process</li> <li>• An awareness campaign should be conducted for the general users of information systems assets</li> </ul>
<b>7.</b>	<b>Perform regular Testing of the BCP</b>
	<ul style="list-style-type: none"> <li>• A proper test plan should be finalized and implemented to ensure its proper functionality and training to the BC team members. The BC Test Plan should specify <ul style="list-style-type: none"> <li>○ the type of test,</li> <li>○ the expected period of recovery,</li> <li>○ frequency for such tests</li> </ul> </li> <li>• The test results should be submitted to the concern authority with an evaluation of the BCP.</li> <li>• The results of the BC tests should be documented and used for fine tuning the BCP.</li> </ul>
<b>8.</b>	<b>Maintain the BCP up-to-date</b>
	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.
<b>9.</b>	<b>Maintain and update contact numbers of BC team members</b>
	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.
<b>10.</b>	<b>Keep supporting documents updated</b>
	<p>To ensure effective business continuity, following documents should be maintained and kept up-to-date :</p> <ul style="list-style-type: none"> <li>• Security registers where all the entries of external parties / contractors etc. in the premises would be logged.</li> <li>• Duly authorized list of personnel who has the access to secure areas.</li> <li>• The recordings stemming from security cameras stored on any media.</li> <li>• Floor plans detailing physical zoning and access controls.</li> </ul>

	<ul style="list-style-type: none"> <li>• Plans of Secure Areas / Computing facilities.</li> <li>• The historical log files of entrances and exits provided by the system console.</li> <li>• Signed and stored contracts / agreements for each external partner which has access to computing facilities.</li> </ul>
<b>11.</b>	<b>Ensure Security of the BC Plan</b>
	BC Plan is a confidential document and hence appropriate access controls should be implemented over the soft and hard copies of the plan.
<b>12.</b>	<b>Audit the BC Plan</b>
	The Business Continuity Management Process and the Business Continuity Plan should be audited to ensure that it meets the guidelines prescribed by the regulatory authorities.

#### 10.2.5 Implementation Responsibilities

- BCP Team
- Departmental Heads

## **34. Vendor Management Policy – make small para**

### **11.1.1 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.

### **11.1.2 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..

### **11.1.3 Policy Statement(s)**

1. Procedures should be established for vendor selection.
2. Agreements are entered into with the vendor.
3. Perform risk assessment of contracts.
4. Deliverables be clearly identified with time lines.
5. Provide for Alternate / Stand by vendor
6. Vendor performance should be monitored.
7. Regular review of vendor contract.
8. Security in Supply Chain Agreements.
9. Obtain Self-Certification from vendors

#### 11.1.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Procedures should be established for vendor selection.</b>
	Define a vendor selection criterion which is based on a comparative analysis of techno-commercials aspects 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.
<b>2.</b>	<b>Agreements are entered into with the vendor.</b>
	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.
<b>3.</b>	<b>Perform risk assessment of contracts.</b>
	A formal Risk Assessment of the contractor / supplier should be carried out before entering into any key / critical / high value contract. The approval / sanction note should consider various parameters for selection as a part of the Risk Assessment of the vendor. A similar risk assessment should be carried out once every year or before renewal of the contract; whichever is applicable.
<b>4.</b>	<b>Deliverables be clearly identified with time lines.</b>
	The service deliverables should be clearly identified with time lines to help monitor the performance. The vendor should prepare a disaster recovery plan to ensure uninterrupted service delivery. The vendor should ensure that its disaster recovery plan is reviewed, updated and tested regularly in accordance with the changes in technology changes as well as operational requirements. All the relevant resources of the vendor should be properly trained in the procedures for invoking the disaster recovery plan.
<b>5.</b>	<b>Provide for Alternate / Stand by vendor</b>
	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.



<b>6.</b>	<b>Vendor performance should be monitored.</b>
	A process should be set up for monitoring the performance against the criteria defined in the SLA. Consider appointing a Relationship manager to coordinate various issues / requirements with the vendor.
<b>7.</b>	<b>Regular Review of Vendor Contract</b>
	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.
<b>8.</b>	<b>Security in Supply Chain Agreements</b>
	<p>The following points (as applicable) should be included in supplier agreements concerning supply chain security:</p> <ul style="list-style-type: none"> <li>• Defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;</li> <li>• For information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;</li> <li>• For information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;</li> <li>• Implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;</li> <li>• Implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;</li> <li>• Obtaining assurance that critical components and their origin can be traced throughout the supply chain;</li> </ul>

	<ul style="list-style-type: none"> <li>• Obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;</li> <li>• Defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;</li> <li>• Implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.</li> </ul>
<b>9.</b>	<b>Obtain Self-Certification from vendors</b>
	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers / Depository Participants are managed by vendors and the Stock Brokers / Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers / Depository Participants should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

#### **11.1.5 Implementation Responsibilities**

- Department Heads
- IT Infrastructure Department
- General Administration Department

## **35. Security Compliance Policy**

### **13.1.1 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.

### **13.1.2 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"**.

### **13.1.3 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

#### 13.1.4 Detailed Procedures

#	Detailed Procedures
<b>1.</b>	<b>Identification of the applicable laws and regulatory guidelines.</b>
	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.
<b>2.</b>	<b>Ensure Implementation of the identified requirements</b>
	<p>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.</p> <p>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.</p>
<b>3.</b>	<b>Ensure Compliance with the Intellectual Property Rights</b>
	<p>Ensure compliance to the IPR provisions by:</p> <ul style="list-style-type: none"> <li>• Using only The Organisation approved software.</li> <li>• Reviewing the Servers and Desktops / laptops for potential violations</li> <li>• Preventing installation of software beyond the number of permitted Licenses</li> </ul> <p>All users should be given awareness that they should not install any unlicensed / warez software.</p>
<b>4.</b>	<b>Comply with guidelines on E-Waste Management.</b>
	<ul style="list-style-type: none"> <li>• Controls as defined in the chapter on E-Waste Management Policy should be implemented.</li> </ul>
<b>5.</b>	<b>Protect Organisational Records</b>
	<ul style="list-style-type: none"> <li>• Appropriate controls should be implemented over the various types of Records, like paper, microfilm, electronic etc.</li> <li>• Data storage system should help in efficiently fetching the required data</li> <li>• Retention periods of various types of records should be defined and adhered to by respective functional / department heads.</li> </ul>
<b>6.</b>	<b>Ensure Data Protection and Privacy of personal information</b>
	<ul style="list-style-type: none"> <li>• The data received from clients and other critical information, should be appropriately "access controlled"</li> </ul>

	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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</li> </ul>
<b>7.</b>	<b>Prevention of misuse of information processing facility</b>
	<ul style="list-style-type: none"> <li>• Users should be given appropriate awareness training that the data or the production facilities are to be used only by the authorised users</li> <li>• 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.</li> </ul> <p>The above awareness would act as a deterrent and help avoid unauthorised access attempts</p>
<b>8.</b>	<b>Compliance with Organisation's information security policies</b>
	<ul style="list-style-type: none"> <li>• At least once a year, the Asset owners should perform reviews of the accesses granted to users.</li> <li>• 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</li> </ul>
<b>9.</b>	<b>Ensure Technical Compliance Checking</b>
	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".
<b>10.</b>	<b>Sharing of Information with SEBI</b>
	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.
<b>11.</b>	<b>Systems Managed by MIIs</b>
	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.

#### **13.1.5 Implementation Responsibilities**

- Compliance Department
- CISO

## **36. ISMS Audit Policy**

### **13.2.1 Policy Objective**

- To ensure that the set up is audited by performing
  - Systems Audits to ensure technical configurations comply with the Cyber Security and Cyber Resilience Policies and Procedures and the Infrastructure hardening guidelines
  - Vulnerability Assessment and Penetration Systems at regular intervals
- Prepare a ISMS Audit Plan for Systems Audits and VA-PT
- Ensure independence of Systems Audit and VA-PT Teams

### **13.2.2 Policy Scope**

This policy covers all information assets supporting the business activities. It covers Business Applications, Databases, Operating Systems, Web Servers, Network Devices, Data Centre and other physical areas, Infrastructure Assets like UPS-Batteries, Air Conditioning, Fire Extinguishers, etc. and USERS.

### **13.2.3 Policy Statement(s)**

1. ISMS audit should be appropriately planned.
2. Cooperate with the Auditors
3. NDA with the Auditor / Firm
4. Ensure independence of the Auditor / Firm.
5. Establish procedures for audit reporting.
6. Audit Findings should be classified according to criticality
7. Establish procedures for correction and corrective actions.

### **13.2.4 Detailed Procedures**

As mentioned above 2 types of ISMS Audits are to be performed as under

#### **1. Systems Audits**

This is a technical area which should be performed by qualified systems auditors like CISAs / DISAs.

The main objective of systems audit is to review the configuration of technical areas like Applications, Databases, Web Servers, Operating Systems, switches-routers-firewalls etc.

This also includes the review of the Physical and Environmental Controls, Status of User Training and Security Education, review of Infrastructure (UPS, Batteries, Air Conditioning Systems, Fire Extinguishers, etc.)

#### **2. Vulnerability Assessment and Penetration Testing**

This is a highly technical area and calls for usage of specialised tools, techniques and should be performed by qualified persons.

Combination of automated tools and manual techniques should be used to perform a comprehensive VA. The VA should be performed from within the Network as well as from outside over the internet as per the features of the Applications and supporting infrastructure.

While performing VA-PT of any information asset, care should be taken to ensure that

- a. A formal confirmation is given to the external firm to perform VA-PT
- b. Appropriate backup is taken, before commencement of VA-PT
- c. The relevant owner and administrator/s are put on alert
- d. A Process should be established to rectify the issues identified in VA and to perform a follow up VA to review the effectiveness of rectifications.

As per the SEBI guidelines the organization has decided

- To perform vulnerability assessment and penetration testing at regular intervals (at least once a year) of their IT environment exposed to the internet.
- To perform vulnerability scanning and conduct penetration testing prior to the commissioning of any new system that is accessible over the internet.
- That in case any vulnerabilities are discovered in "off-the-shelf" products (used for core business) or applications provided by exchange empanelled vendors, those will be reported to the vendors and the exchanges in a timely manner.

That remedial actions will be immediately performed to address the observations / gaps that are identified during vulnerability assessment and penetration testing.



#	Detailed Procedures
<b>1.</b>	<b>ISMS Audit should be appropriately Planned</b>
	<p>CISO / Designated Officer should prepare a detailed ISMS Audit Plan every year and ensure that all critical information assets are covered with the above described approach. These audits should be preferably conducted prior to the statutory audit (as applicable).</p> <p>The ISMS audit calendar should be planned and scheduled in such a way that the audits should not become hindrance to the day-to-day operations of the business.</p> <p>The auditor and auditee should be given adequate notice about the audit.</p>
<b>2.</b>	<b>Cooperate with the Auditors</b>
	<p>Auditors should be granted access to all the relevant information assets, records, personnel, and properties.</p> <p>However the Auditee may choose to prohibit access to the auditors to certain highly confidential areas like intellectual properties, trade secrets, Salary and commission details etc.</p>
<b>3.</b>	<b>NDA with the Auditors</b>
	Appropriate NDA should be entered into with the Auditor / Firm
<b>4.</b>	<b>Ensure independence of the Auditor / Firm</b>
	While Engaging auditor / Firm it should be ensured that the Auditor is "INDEPENDENT" of the area under audit.
<b>5.</b>	<b>Establish procedures for Audit Reporting</b>
	<p>ISMS Audit Reports giving details of the findings should be submitted to the CISO / Designated Officer / Systems Audit Head for rectification (Correction ) and improvement in the controls (corrective action).</p> <p>After follow up audit and VA-PT, the Reports should be presented to the Proprietor / Partners /Board / Management.</p>
<b>6.</b>	<b>Audit Findings should be classified according to criticality</b>
	<p>The findings of ISMS Audits should be classified as follows:</p> <ul style="list-style-type: none"> <li>• <b>Complied</b> : Where the area under audit complies with procedure/s or Management System requirement/s</li> <li>• <b>Partially Complied</b> : An isolated incident of a failure to comply with a procedure or Management System requirement</li> <li>• <b>Not Complied</b> : A failure or complete omission of a requirement</li> <li>• <b>Not Applicable</b> : Where the control being considered is not applicable to the area under audit</li> </ul>

<b>7.</b>	<b>Establish procedures for correction and corrective actions.</b>
	<p>The observations raised in the ISMS Audits should be studied, classified based on their severity and taken up for rectification. This study also involves a systematic investigation of the "ROOT CAUSE" of identified problems or identified risks, with an objective to correct them (correction) and improve the control (corrective action).</p> <p>The Auditee should prepare a report mentioning target dates of correction / corrective action (where immediate correction / corrective action is not immediately possible) for the audit findings. Thereafter, these reports should be submitted to the Information Security Committee for review and further actions (if required).</p>

#### **13.2.6 Implementation Responsibilities**

- Department Heads
- Information Security Committee

## **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 12<sup>th</sup> May 2011.