



CIN : U65990WB2009PLC138910

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN DP 299-2016

## **POLICY ON CYBER SECURITY AND CYBER RESILIENCE**

### **Introduction**

We, Achiivers Equities Limited (**the "Company"**), being a brokerage house, provides services to our customers. Therefore, it is necessary to have a robust cyber security and cyber resilience framework in order to provide essential facilities, perform critical functions systematically relating to securities market and to protect the data from cyber-attacks and cyber threats.

In view of the above circumstances and to strengthen the cyber security framework, the Company revised its Policy on Cyber Security and Cyber Resilience at its Board Meeting dated 21 December, 2019 which will come into effect on immediate basis.

### **Background**

SEBI has issued circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated 03 December, 2018 and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated 15 October, 2019, providing guidelines on Cyber Security and Cyber Resilience. The objective of the said circular is to adapt to the rapid technological developments in Securities Market which have highlighted the need for robust Cyber and Cyber Resilience at the level of Stock brokers/Depository participants who are performing significant functions in providing services to the holder of Securities.

In order to protect the integrity of data and guard against breaches of Privacy and to comply with the applicable regulations, Achiivers Equities Ltd has framed a policy for implementation to meet the objectives.

### **Date of Implementation of the Circular**

Circular shall come into effect on immediate basis.

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

For Achiivers Equities Ltd.

Director





**National Stock Exchange (NSE)**  
SEBI Regn. No.: INZ000217438  
**IRDAI**  
Regn. No.: CA0596

**CIN : U65990WB2009PLC138910**

**Bombay Stock Exchange (BSE)**  
SEBI Regn. No.: INZ000217438  
**CDSL**  
SEBI Regn. No.: IN-DP-299-2016

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

**Governance**

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

- Identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:
  - 'Identify' critical IT assets and risks associated with such assets.
  - 'Protect' assets by deploying suitable controls, tools and measures.
  - 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes.
  - 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.
  - 'Recover' from incident through incident management and other appropriate recovery mechanisms.
  
- As a Stock broker trading through APIs based terminal or acting as a depository Participants should refer best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
  - ISO 27001 is an international standard for the establishment, implementation, maintenance, and continual improvement of an Information Security Management System. The standard is a joint effort by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).
  - COBIT 5 is a framework from the Information Systems Audit and Control Association (ISACA) for the management and governance of information technology (IT). ... Achieve strategic goals by using IT assistance. Maintain operational excellence by using technology effectively. Keep IT-related risk at an acceptable level.
  - The main benefit of implementing ISO 27001 is a systemic Information Security Management System that helps with the identification of critical information, the information security risk assessment of the system, and the implementation of security controls, all of which help to create a secure culture in the organization.
  - ISO 27001 is beneficial for the organization in terms of its security.

For Achievers Equities Ltd  
*[Signature]*  
Director

CIN : U65990WB2009PLCI38910

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

- The five COBIT 5 principles are:
- Meeting stakeholder needs
  - Covering the enterprise end to end
  - Applying a single integrated framework
  - Enabling a holistic approach
  - Separating governance from management

- We have designated Mr. Pankaj Kumar Das, Compliance Officer to assess, identify, and reduce security and Cyber Security risks, respond to incidents establish appropriate standards and controls and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.
- A reporting procedure has been designed to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
- The Designated officer and the technology committee will periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

### **Identification**

- We have identified critical assets based on their Sensitivity and criticality for business operations, services and data management. Maintenance of up-to-date inventory of the hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows. Accordingly identify cyber risks, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

### **Protection**

#### **Access controls:**

- Any access to systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. To identify the access we have granted access to IT systems, applications, databases

For Achievers Equities Ltd

  
Director





AN ISO 9001:2008 CERTIFIED COMPANY

CIN : U65990WB2009PLC138910

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

and networks on a need-to-use basis and based on the principle of least privilege. Implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases.

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

**Physical Security:**

- Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees. Access should be revoked immediately if the same is no longer required.
- Office premises should be physically secured and monitored by security guards.

**Network Security Management:**

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

**Data security:**

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

For Achievers Equities Ltd

Director



CIN : U65990WB2009PLC138910

**National Stock Exchange (NSE)**  
SEBI Regn. No. : INZ000217438  
**IRDAI**  
Regn. No. : CA0596

**Bombay Stock Exchange (BSE)**  
SEBI Regn. No. : INZ000217438  
**CDSL**  
SEBI Regn. No. : IN-DP-299-2016

**Hardening of Hardware and Software:**

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

**Application Security in Customer Facing Applications:**

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

**Patch management:**

- Patch management procedures should include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner. Testing to be performed on security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

**Disposal of data, systems and storage devices:**

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

**Vulnerability Assessment and Penetration Testing (VAPT):**

- Regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.

For Achievers Equities Ltd.

*[Handwritten Signature]*  
Director



CIN : U65990WB2009PLC138910

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

• Systems which are publicly available over the internet should also carry out penetration tests, at least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet. Additionally perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.

### **Monitoring and Detection:**

- Establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/ alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.
- Ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.

### **Response and Recovery:**

- Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of Cyber-attack or breach, mitigate its effect and eradicate the incident.
- The response and should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Stock Brokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time.

For Achievers Equities Ltd



Director



CIN : U65990WB2009PLC138910

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

### Sharing of Information:

- Quarterly reports containing information on cyber-attacks and threats measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants.

### Training and Education

- Entities should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. Where possible, this should be extended to outsourced staff, vendors etc.
- The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.

### Systems managed by vendors, MIIs

- As a Stock Broker / Depository Participant we have instructed the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

### Periodic Audit

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

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

For Achievers Equities Ltd.

Director





CIN : U65990WB2009PLC138910

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

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

- Protection of Critical Information Infrastructure (CII) is of paramount concern to governments worldwide. To address this threat, the Government of India has notified the 'National Critical Information Infrastructure Protection Centre' (NCIIPC) as the nodal agencies vide Gazette of India notification on 16th January 2014.
- NCIIPC is driven by its mission to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders with a vision to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country. To achieve this, it is essential to ensure that relevant security mechanisms are built into Critical Information Infrastructure as key design features.
- The National Security Advisor had in July 2013 released a document listing forty controls and corresponding guiding principles for the protection of CIIs. In view of the dynamic nature of cyberspace and to ensure the continued relevance of these controls, NCIIPC is continuously reassessing these based on ongoing experience as well as feedback from NCII constituents, these controls have been grouped into five sets (or families). While all Controls in a family may not be relevant to a particular organization / infrastructure, it is important that conscious sign off (on both, controls implemented, as well as dropped) is taken from senior management based on residual risk acceptable to the Organization.
- **The five families of controls are:**
  - Planning Controls for ensuring that the security is taken as a key design parameter for all new CIIs at conceptualisation and design level itself.
  - Implementation Controls for translating the design/conceptualisation planning into mechanisms for protecting the CII. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.
  - Operational Controls for ensuring that the desired security posture is maintained in the operational environment. These controls also come into play in case of retrofitting existing, unprotected / poorly protected CII.
  - Disaster Recovery/ Business Continuity Planning (BCP) Controls for ensuring minimum downtime and the restoration process.
  - Reporting and Accountability Controls for ensuring adequate accountability and oversight exercised by Senior management, as well as reporting to concerned Government agencies where required enforced through compliance controls.

For Achievers Equities Ltd.

Director



**CIN : U65990WB2009PLC138910**

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

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

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

**For Achievers Equities Ltd**

For Achievers Equities Ltd



Director

**Suman Chakraborty**

**Director**

**Dated:- 21 December, 2019**



**RETENTION AND DISPOSAL POLICY**

**Purpose:**

The purpose of this policy is to detail the procedures for retention and disposal of information to ensure that we carry this out consistently and that we fully document any actions taken. Unless otherwise specified the retention and disposal policy refers to both hard and soft copy documents.

**Review**

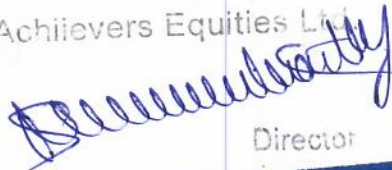
Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

**How long we should keep our paper records**

- Records should be kept for as long as they are needed to meet the operational needs of the Authority, together with legal and regulatory requirements. We have assessed our records to:
  - Determine their value as a source of information about the Authority, its operations, relationships and environment
  - Assess their importance as evidence of business activities and decisions
  - Establish whether there are any legal or regulatory retention requirements
- Where records are likely to have a historical value, or are worthy of permanent preservation, we will transfer them to the National Archives after 25 years.

**Disposal schedule**

- A disposal schedule is a key document in the management of records and information.
- Records on disposal schedules will fall into three main categories:
  - Destroy after an agreed period – where the useful life of a series or collection of records can be easily predetermined (for example, destroy after 3 years; destroy 2 years after the end of the financial year).
  - Automatically select for permanent preservation – where certain group of records can be readily defined as worthy of permanent preservation and transferred to an archive.
  - Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.
- Records can be destroyed in the following ways:
  - ✓ **Destruction**
    - Non-sensitive information – can be placed in a normal rubbish bin
    - Confidential information – cross cut shredded and pulped or burnt
    - Highly Confidential information – cross cut shredded and pulped or burnt
  - Electronic equipment containing information - destroyed using kill disc and for individual folders, they will be permanently deleted from the system.
  - Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.
  - Archival transfer
    - This is the physical transfer of physical records to a permanent custody at the National Archives Office.

For Achievers Equities Ltd  
  
 Director



**CIN : U65990WB2009PLC138910**

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

**Sharing of information**

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

- Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retained in accordance with the guidelines mentioned above. Care should be taken that seemingly duplicate records have not been annotated.
- Where we share information with other bodies, we will ensure that they have adequate procedures for records to ensure that the information is managed in accordance with the Authority's policies, relevant legislation and regulatory guidance.
- Where relevant to do so we will carry out a data privacy impact assessment and update our privacy notices to reflect data sharing.

#### **An audit trail**

- You do not need to document the disposal of records which have been listed on the records retention schedule. Documents disposed out of the schedule either by being disposed of earlier or kept for longer than listed will need to be recorded for audit purposes.
- This will provide an audit trail for any inspections conducted by the regulatory and will aid in addressing Freedom of Information requests, where we no longer hold the material.

#### **Monitoring**

- Responsibility for monitoring the disposal policy rests with the designated officer. The policy will be reviewed annually or more often as required.

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

For Achievers Equities Ltd

For Achievers Equities Ltd

  
\_\_\_\_\_  
**Suman Chakraborty**  
Director

**Dated: 21 December, 2019**



**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

## **ELECTRONIC STORAGE MEDIA DISPOSAL POLICY**

### **Purpose:**

The purpose of this policy is to define standards for proper data sanitization and/or disposal of electronic storage media that has (or may have) contained personal information at the Company's end.

### **General/Definitions:**

• **Electronic Storage Media** - Any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP disks, magnetic tapes and SD cards.

• **Personal information** - An individual's first name and last name or first initial and last name in combination with one or more of the following data elements: social security number, driver's license number or state-identification card number, or financial account number, or credit or debit card number, with or without any required security code, access code, personally identifiable identification number or password, that would permit access to a resident's financial account.

• **Sensitive Information** - Data whose disclosure would not result in any business, financial or legal loss but involves issues of personally identifiable credibility, privacy or reputation. The security and protection of this data is dictated by a desire to maintain staff and student privacy.

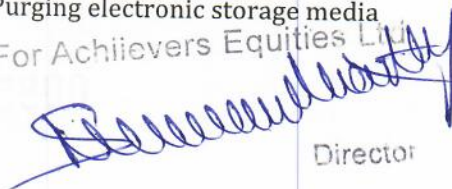
#### • **Sanitizing Storage Media** -

➤ Disposal is defined as the act of discarding media with no other sanitization considerations. Examples of Disposal include discarding paper in a recycling container, deleting electronic documents using standard file deletion methods and discarding electronic storage media in a standard trash receptacle.

➤ Clearing is defined as a level of sanitization that renders media unreadable through normal means. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Clearing prevents data from being recovered using standard disk and file recovery utilities.

➤ Purging is defined as a more advanced level of sanitization that renders media unreadable even through an advanced laboratory process. In traditional thinking, Purging consists of using specialized utilities that repeatedly overwrite data; however, with advancements in electronic storage media, the definitions of Clearing and Purging are converging. For example, Purging a hard drive manufactured after 2001 only requires a single overwrite. For the purpose of this Policy, Clearing and Purging will be considered the same. Degaussing is also an acceptable method of Purging electronic storage media.

For Achievers Equities Ltd



Director





CIN : U65990WB2009PLC138910

National Stock Exchange (NSE)

SEBI Regn. No. : INZ000217438

IRDAI

Regn. No. : CA0596

Bombay Stock Exchange (BSE)

SEBI Regn. No. : INZ000217438

CDSL

SEBI Regn. No. : IN-DP-299-2016

➤ Destroying is defined as rendering media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting. This is a common sanitization method for single-write storage media such as a CD or DVD for which other sanitization methods would be ineffective. This is also a common practice when permanently discarding hard drives.

**Organizational Scope:**

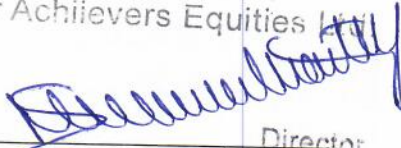
This policy applies to all personnel who have responsibility for handling and proper disposal of electronic storage media at Company.

**Policy Content and Guidelines:**

- All electronic storage media should be sanitized (Cleared/Purged) prior to sale, donation, being moved to unsecured storage (for spare parts), or transfer of ownership. A transfer of ownership may include transitioning media to another individual or department at the Company or replacing media as part of a lease agreement.
- All electronic storage media must be destroyed when it has reached the end of its useful life and/or when other sanitizing methods are not effective (e.g. single-write media or media that is permanently write protected), provided that the destruction does not conflict with Company data retention policies or any regulatory requirements (e.g. electronic discovery).

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

For Achievers Equities Ltd

For Achievers Equities Ltd  


Director

Suman Chakraborty

Director

Dated: 21 December, 2019





**National Stock Exchange (NSE)**  
SEBI Regn. No. : INZ000217438  
**IRDAI**  
Regn. No. : CA0596

**CIN : U65990WB2009PLC138910**

**Bombay Stock Exchange (BSE)**  
SEBI Regn. No. : INZ000217438  
**CDSL**  
Regn. No. : IN-DP-299-2016

## **INFORMATION SECURITY POLICY**

### **Purpose**

The purpose of this Policy is to safeguard information belonging to the Company and its stakeholder (third parties, clients or customers and the general public), within a secure environment.

This Policy informs the Company's staff, and other external Vendors entitled to use Company facilities, of the principles governing the holding, use and disposal of information.

### **It is the goal of the Company that:**

- Information will be protected against unauthorised access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this Policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the Director of ICT Systems, and investigated through the appropriate management channel.

### **Information relates to:**

- Electronic information systems (software, computers, and peripherals) owned by the Company whether deployed or accessed on or off campus.
- The Company's computer network used either directly or indirectly.
- Hardware, software and data owned by the Company.
- Paper-based materials.
- Electronic recording devices (video, audio, CCTV systems).

### **The Policy**

The Company requires all users to exercise a duty of care in relation to the operation and use of its information systems.

### **Authorised users of information systems**

- With the exception of information published for public consumption, all users of Company information systems must be formally authorised by appointment as a member of staff, or by other process specifically authorised by the designated officer. Authorised users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person. The "Network password policy" describes these principles in greater detail.

For Achiivers Equities Ltd





**National Stock Exchange (NSE)**  
SEBI Regn. No. : INZ000217438  
**IRDAI**  
Regn. No. : CA0596

**CIN : U65990WB2009PLC138910**  
**Bombay Stock Exchange (BSE)**  
SEBI Regn. No. : INZ000217438  
**CDSL**  
SEBI Regn. No. : IN-DP-299-2016

- Authorised users will pay due care and attention to protect Company information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:
  - permission of the information owner
  - the risks associated with loss or falling into the wrong hands
  - How the information will be secured during transport and at its destination.

**Acceptable use of information systems**

- Use of the Company's information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the list of subsidiary policies.

**Information System Owners**

- Designated Officer/Chief Technology Officer/Directors who are responsible for information systems are required to ensure that:
  - Systems are adequately protected from unauthorised access.
  - Systems are secured against theft and damage to a level that is cost-effective.
  - Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
  - Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
  - Data is maintained with a high degree of accuracy.
  - Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
  - Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
  - Any third parties entrusted with Company data understand their responsibilities with respect to maintaining its security.

**Personal Information**

- Authorised users of information systems are not given rights of privacy in relation to their use of Company information systems. Duly authorised officers of the Company may access or monitor personal data contained in any Company information system (mailboxes, web access logs, file-store etc.).
- Individuals in breach of this policy are subject to disciplinary procedures at the instigation of the Designated Officer with responsibility for the relevant information system, including referral to the Police where appropriate.
- The Company will take legal action to ensure that its information systems are not used by unauthorised persons.

For Achievers Equities Ltd  
*[Handwritten Signature]*





**National Stock Exchange (NSE)**  
SEBI Regn. No.: INZ000217438  
**IRDAI**  
Regn. No.: CA0596

**CIN : U65990WB2009PLC138910**

**Bombay Stock Exchange (BSE)**  
SEBI Regn. No.: INZ000217438  
**CDSL**  
SEBI Regn. No.: IN-DP-299-2016

**Ownership**

- The Designated Officer of ICT Systems has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.
- Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.

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

**For Achiivers Equities Ltd**

For Achiivers Equities Ltd  
  
Director

**Suman Chakraborty**  
Director

**Dated: 21 December, 2019**



**National Stock Exchange (NSE)**  
SEBI Regn. No. : INZ000217438  
**IRDAI**  
Regn. No. : CA0596

**CIN : U65990WB2009PLC138910**

**Bombay Stock Exchange (BSE)**  
SEBI Regn. No. : INZ000217438  
**CDSL**

SEBI Regn. No. : IN-DP-299-2016

**INTERNET ACCESS POLICY**

**Objective:**

Achiivers Equities Ltd recognizes that use of the Internet and e-mail is necessary in the workplace, and employees are encouraged to use the Internet and e-mail systems responsibly, as unacceptable use can place Company and others at risk. This policy outlines the guidelines for acceptable use of Company's technology systems.

**Scope:**

This policy must be followed in conjunction with other policies governing appropriate workplace conduct and behaviour. Any employee who abuses the company-provided access to e-mail, the Internet, or other electronic communications or networks, including social media, may be denied future access and, if appropriate, be subject to disciplinary action up to and including termination. Company complies with all applicable central, state and local laws as they concern the employer/employee relationship, and nothing contained herein should be misconstrued to violate any of the rights or responsibilities contained in such laws.

Questions regarding the appropriate use of Company's electronic communications equipment or systems, including e-mail and the Internet, should be directed to your supervisor or the information technology (IT) department.

**Policy:**

Company has established the following guidelines for employee's use of the company's technology and communications networks, including the Internet and e-mail, in an appropriate, ethical and professional manner.

**Confidentiality and Monitoring**

- All technology provided by Company, including computer systems, communication networks, company-related work records and other information stored electronically, is the property of the Company and not the employee. In general, use of the company's technology systems and electronic communications should be job-related and not for personal convenience. Company reserves the right to examine, monitor and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite.
- Internal and external e-mail, voice mail, text messages and other electronic communications are considered business records and may be subject to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the company.

**Appropriate Use**

- Company employees are expected to use technology responsibly and productively as necessary for their jobs. Internet access and e-mail use is for job-related activities; however, minimal personal use is acceptable.

For Achiivers Equities Ltd.





CIN : U65990WB2009PLC138910

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

- Employees may not use Company's Internet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference may be transmitted. Harassment of any kind is prohibited.
- Disparaging, abusive, profane or offensive language and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or e-mail—are forbidden.
- Copyrighted materials belonging to entities other than Company may not be transmitted by employees on the company's network without permission of the copyright holder.
- Employees may not use Company's computer systems in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and spamming (sending unsolicited e-mail to thousands of users).
- Employees are prohibited from downloading software or other program files or online services from the Internet without prior approval from the IT department. All files or software should be passed through virus-protection programs prior to use. Failure to detect viruses could result in corruption or damage to files or unauthorized entry into company systems and networks.
- Every employee of Company is responsible for the content of all text, audio, video or image files that he or she places or sends over the company's Internet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. Company's corporate identity is attached to all outgoing e-mail communications, which should reflect corporate values and appropriate workplace language and conduct.

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

For Achiivers Equities Ltd

For Achiivers Equities Ltd

Director

**Suman Chakrbraty**

Director

Dated: 21 December, 2019





CIN : U65990WB2009PLC138910

National Stock Exchange (NSE)

SEBI Regn. No. : INZ000217438

IRDAI

Regn. No. : CA0596

Bombay Stock Exchange (BSE)

SEBI Regn. No. : INZ000217438

CDSL

SEBI Regn. No. : IN-DP-299-2016

**IT ACCESS CONTROL AND USER ACCESS MANAGEMENT POLICY:**

**Policy Statement:**

- Protecting access to IT systems and applications is critical to maintain the integrity of the Company's technology and data and prevent unauthorized access to such resources.
- Access to Company's systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

**Background**

- Access controls are necessary to ensure only authorized users can obtain access to the Company's information and systems.
- Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job related duties.

**Policy Objective**

- The objective of this policy is to ensure the Institution has adequate controls to restrict access to systems and data.

**Scope**

- This policy applies to all branch and head office including employees, Consultants and Outside Vendors accessing Company's IT systems and applications.

**Definitions**

- "Access Control" is the process that limits and controls access to resources of a computer system.
- "Users" are employees, consultants, contractors, agents and authorized users accessing Company IT systems and applications.
- "System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications.
- "Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.

For Achievers Equities Ltd  
*[Signature]*  
Director



CIN : U65990WB2009PLC138910

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

- "Access Privileges" are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

- "Administrator Account" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.
- "Application and Service Accounts" are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.
- "Nominative User Accounts" are user accounts that are named after a person.
- "Non-disclosure Agreement" is a contract between a person and the Company stating that the person will protect confidential information (as defined in the Record Classification and Handling Policy) covered by the contract, when this person has been exposed to such information.

### Guiding Principles - General Requirements

- The Company will provide access privileges to Company technology (including networks, systems, applications, computers and mobile devices) based on the following principles:
  - **Need to know** - users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.
  - **Least privilege** - users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.
- Requests for users' accounts and access privileges must be formally documented and appropriately approved.
- Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by the system owner.
- Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only.
- Where possible, the Company will set user accounts to automatically expire at a pre-set date. More specifically,
  - When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.
  - User accounts assigned to contractors will be set to expire according to the contract's expiry date.

For Achievers Equities Ltd.



Director



CIN : U65990WB2009PLC138910

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

➤ ~~User accounts will be disabled after 3 months of inactivity. This does not apply to accounts assigned to employees.~~

- User accounts with signed contracts for a recurring, continuing, or tenure track appointment for an upcoming term can be active for up to four months between appointments.
- Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access Company's systems.
- A verification of the user's identity must be performed by the IT Director, Help Desk, or designate before granting a new password.
- Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:
  - An active account assigned to external contractors, vendors or employees that no longer work for the Company.
  - An active account with access rights for which the user's role and responsibilities do not require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.
  - System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
  - Unknown active accounts.
- All access requests for system and application accounts and permissions will be documented using the ticketing system in place.

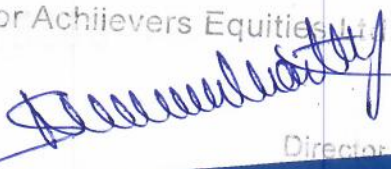
### Guiding Principles - Privileged Accounts

- A nominative and individual privileged user account must be created for administrator accounts (such as "first\_name.last\_name.admin"), instead of generic administrator account names.
- Privileged user accounts can only be requested by managers or supervisors and must be appropriately approved.

### Guiding Principles - Shared User Accounts

- Where possible, the use of specific network domain "security groups" should be used to share common access permissions across many users, instead of shared accounts.
- Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as "guest" and "functional" accounts.

For Achievers Equities Ltd.



Director



CIN : U65990WB2009PLC138910

**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

**When shared accounts are required:**

- Passwords will be stored and handled in accordance with the Password Policy.
- The use of shared accounts will be monitored where possible, including the recording of the time of access, the reason for accessing the shared user account, and the individual accessing his account. When the shared user account has administrative privileges, such a procedure is mandatory and access to the monitoring logs must be protected and restricted.

**Vendor or Default User Accounts**

- Where possible, all default user accounts will be disabled or changed. These accounts include “guest”, “temp”, “admin”, “Administrator”, and any other commonly known or used default accounts, as well as related default passwords used by vendors on “commercial off-the-shelf” systems and applications.

**Test Accounts**

- Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request to the IT Director or the IT Help Desk.
- Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.
- Test accounts will be disabled / deleted when they are no longer necessary.

**Contractors and Vendors**

- In accordance with the Contract Management Policy, contracts with contractors / vendors will include specific requirements for the protection of data. In addition, contractor / vendor representatives will be required to sign a Non-disclosure Agreement (“NDA”) prior to obtaining approval to access Institution systems and applications.
  - Prior to granting access rights to a contractor / vendor, the IT Director or Help Desk must verify the requirements of Section 11.1 have been complied with.
  - The name of the contractor / vendor representative must be communicated to the IT Help Desk at least 2 business days before the person needs access.
- The Company will maintain a current list of external contractors or vendors having access to Company’s systems.
- The need to terminate the access privileges of the contractor / vendor must be communicated to the IT Help Desk at least 1 business day before the contractor / vendor representative’s need for such access ends.

For Achievers Equities Ltd  
  
Director





**National Stock Exchange (NSE)**  
SEBI Regn. No. : INZ000217438  
**IRDAI**  
Regn. No. : CA0596

**CIN : U65990WB2009PLC138910**

**Bombay Stock Exchange (BSE)**  
SEBI Regn. No. : INZ000217438  
**CDSL**  
SEBI Regn. No. : IN-DP-299-2016

**Access Control Requirements**

- All users must use a unique ID to access Company's systems and applications. Passwords must be set in accordance with the Password Policy.
- Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.
  - Remote access to Company's systems and applications must use two-factor authentication where possible.
  - System and application sessions must automatically lock after 15 minutes of inactivity.

**Roles and Responsibilities**

STAKEHOLDER	RESPONSIBILITIES
Board of Director	<ul style="list-style-type: none"> <li>• Approve and formally support this policy.</li> </ul>
President, Administration	<ul style="list-style-type: none"> <li>• Review and formally support this policy.</li> </ul>
IT Director/Designated officer	<ul style="list-style-type: none"> <li>• Develop and maintain this policy.</li> <li>• Review and approve any exceptions to the requirements of this policy.</li> <li>• Take proactive steps to reinforce compliance of all stakeholders with this policy.</li> </ul>
Supervisors or Company's Representative	<ul style="list-style-type: none"> <li>• Support all employees and others in the understanding of the requirements of this policy.</li> <li>• Immediately assess and report to the IT service desk any non-compliance instance with this policy.</li> </ul>
Contract Administrators	<ul style="list-style-type: none"> <li>• Ensure that the responsibilities and security obligations of each party to the contractual relationship are outlined in the contract executed between the Company's and the contractor/sub-contractor.</li> </ul>
Human Resources	<ul style="list-style-type: none"> <li>• Present each new employee or contractor with the relevant Company's IT and Security Policies, upon the first day of commencing work with Company's.</li> <li>• Support all employees and other in the understanding of the requirements of this policy.</li> </ul>
All users (Employees and contractors, Visitors and or Volunteers)	<ul style="list-style-type: none"> <li>• Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Company's Representative as soon as possible.</li> </ul>

For Achievers Equities Ltd.

*[Handwritten Signature]*  
Director





**National Stock Exchange (NSE)**

SEBI Regn. No. : INZ000217438

**IRDAI**

Regn. No. : CA0596

**CIN : U65990WB2009PLC138910**

**Bombay Stock Exchange (BSE)**

SEBI Regn. No. : INZ000217438

**CDSL**

SEBI Regn. No. : IN-DP-299-2016

**Exceptions to the Policy**

- Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Director/Designated Officer.
- **Policy exceptions must describe:**
  - The nature of the exception
  - A reasonable explanation for why the policy exception is required
  - Any risks created by the policy exception
  - Evidence of approval by the IT Director
- **Inquiries**
  - Inquiries regarding this policy can be directed to the IT Director/Designated officer.

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

**For Achiivers Equities Ltd**

For Achiivers Equities Ltd.

Director

**Suman Chakraborty**

**Director**

**Dated: 21 December, 2019**