ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

USE MANAGEMENT & ACCESS CONTROL POLICY

Version	2024/01.02
Review Date	05/04/2024
Review & Approved by	Reviewed by Technology Committee & Approved by Board of Directors

1 Overview

Access control standards for information systems must be established by management and shall incorporate the need to balance restrictions to prevent unauthorized access against the need to provide unhindered access to meet business needs.

2 Scope

Access to all systems must be authorised by the owner of the system and such access, including the appropriate access rights (or privileges) must be recorded in an Access Control List. Such records are to be regarded as Highly Confidential documents and safeguarded accordingly

3 Purpose

The purpose of the Access Control Policy is to define a set of computer connection classes, designed to minimize the exposure to company from destruction, theft and loss of data (eg. confidentiality and privacy), disruption to business operations, and damage to the corporate image which may follow from unauthorized use of its electronic resources.

4 Policy

4.1 Access to the resources on the network must be strictly controlled to prevent unauthorized access.

4.2 Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

4.3 Connections to the network (including users' logon) have to be properly managed to ensure that only authorised devices / persons are connected.

4.4 Access to operating system is to be restricted to those persons who are authorised to perform systems administration/management functions

4.5 Physical access to high security areas is to be controlled with strong identification and authentication techniques.

4.6 Access controls has to be set at an appropriate level which minimizes information security risks

4.7 Access to systems and their data must be restricted to ensure that information is denied to unauthorized users.

4.8 Access is to be logged and monitored to identify potential misuse of systems or information

4.9 Access to information and documents is to be carefully controlled, ensuring that only authorised personnel may have access to sensitive information

4.10 Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques

4.11 Passwords must not be placed in emails unless they have been encrypted

4.12 Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured

4.13 Activities performed as administrator or super user must be logged where it is feasible to do so.

4.14 Personnel who have administrative system access shall use other less powerful accounts for performing non-administrative tasks. There shall be a documented procedure for reviewing system logs.

5 Extension of IS policy to Vendors/ Service Providers

5.1 Whenever any third party is signed for procuring software or database support care shall be taken that there is no data leakage

5.2 The vendor shall not be allowed to their presentations or demonstrations on the company terminals.

6 Employee Roles and Responsibilities

a. IT Manager/Systems Administrator

- Responsibilities:
- Oversee user management and access control processes.
- Define user roles and access privileges based on job functions.
- Provision user accounts and grant access to systems and networks.
- Implement and enforce password policies and security measures.
- Monitor user activity logs for suspicious or unauthorized behaviour.
- Conduct regular access reviews and audits to ensure compliance.
- Coordinate with IT support for user on-boarding and off-boarding.
- Stay updated on user management best practices and emerging technologies.

b. Admin Manager/ Officer

- Responsibilities:
- Collaborate with IT and managers to identify user roles and access needs.
- Initiate user provisioning and de-provisioning upon hiring or termination.
- Maintain employee records and track user access requests and approvals.
- Provide user information to IT for account creation and access setup.
- Coordinate with IT to ensure timely user access changes and updates.
- Ensure compliance with data protection regulations.
- Collaborate with IT during employee on-boarding and off-boarding processes.
- Participate in training and awareness programs related to user management.

c. Department Head

- Responsibilities:
- Identify and document access requirements for team members.
- Review and approve access requests for their respective teams.
- Ensure access privileges align with employees' job functions.
- Collaborate with IT and HR to update access privileges as needed.
- Monitor user access and activity within their departments.
- Report any user access violations or suspicious behaviour to IT or HR.
- Promote user awareness and compliance with access control policies.
- Participate in user access audits and reviews.

d. Vendor Relationship Manager

- Responsibilities:
- Manage relationships with external vendors and service providers.

- ➤ Define and document access requirements for vendor employees.
- ➤ Coordinate with IT and Admin for user provisioning and access setup.
- ➤ Monitor vendor employee access and compliance with policies.
- ➤ Conduct periodic reviews of vendor user access and privileges.
- ➤ Address any access-related issues or concerns with vendors.
- ➤ Ensure vendors adhere to data protection and security standards.
- ➤ Collaborate with IT and legal teams for vendor contract negotiations.

e. CISO

Responsibilities:

- ➤ Assist in conducting regular security assessments and audits.
- ➤ Identify access control vulnerabilities and recommend improvements.
- ➤ Assist in designing and implementing access control policies and procedures.
- ➤ Provide training and awareness sessions on access control best practices.
- ➤ Stay updated on emerging security threats and access control technologies.
- ➤ Collaborate with IT and management to respond to security incidents.
- ➤ Review and update user management and access control policies.
- ➤ Participate in security incident response and escalation procedures.

f. Support Staff

Responsibilities:

- ➤ Assist users with access-related issues and inquiries.
- ➤ Respond to access request tickets and provide appropriate access support.
- ➤ Verify user identity and authorization for access changes or resets.
- ➤ Escalate access-related issues to IT administrators as needed.
- ➤ Maintain documentation and knowledge base for access-related procedures.
- ➤ Collaborate with IT administrators to troubleshoot access problems.
- ➤ Participate in user awareness programs regarding access control

Read

7. Access Matrix: (refer Annexure 1)

Review and update
This policy shall be reviewed and updated on an annual basis or on any special event or circumstance

Matrix	IT Head	IT Manager	CISO	Director	Risk Manager	Admin	Back office Executive	Account Executive	Demat Pay in Payout Executive	DP Executive	DP Head	Compliance Officer	Dealer
Trading Application	Read	Read/ Write	Read	Read	Read/ Write	Read	No Access	No Access	No Access	No Access	No Access	Read	Read/ Write
Back Office Application	Read	Read	Read	Read	Read	Read	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read	No Access
Exchange Portal Login	No Access	No Access	No Access	Read	Read	Read	No Access	No Access	No Access	No Access	No Access	Read/ Write	No Access
Firewall	Read	Read	Read	Read	Read	Read	No Access	No Access	No Access	No Access	No Access	Read	No Access
Anti-virus	Read	Read	Read	Read	Read	Read	No Access	No Access	No Access	No Access	No Access	Read	No Access
VPN	Read	Read	Read	Read	Read	Read	No Access	No Access	No Access	No Access	No Access	Read	No Access
DP CDAS System	Read	Read	Read	Read	Read	Read	No Access	No Access	Read	Read/ Write	Read/ Write	Read	No Access
Back Office Database	Read	Read	Read	Read	Read	Read	Read	Read	Read	Read	No Access	Read	No Access
Front Office Database	Read	No Access	Read	No Access	Read	Read	No Access	No Access	No Access	No Access	No Access	Read	No Access
Mail Server	Read	Read	Read	Read	Read	Read	No Access	No Access	No Access	No Access	No Access	Read	No Access
Web Server	Read	Read	Read	Read	Read	Read	No Access	No Access	No Access	No Access	No Access	Read	No Access
Office Application	Read	Read	Read	Read	Read	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	No Access