ANJANEY STOCK BROKING LIMITED

MEMBER: NSE, BSE

DP: NSDL

SEBI SINGLE REG NO. INZ000263532

DP SEBI REG NO. IN-DP-303-2016

TM ID : NSE-12417; BSE-6224

DP ID : IN304012

IT ACCESS CONTROL AND USER ACCESS MANAGEMENT POLICY

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Policy created by	Mr. Pramod Kumar Sanganeria
Policy reviewed by	Technology Committee
Policy reviewed on	30-12-2023
Policy Approved by	Board of Directors
Policy approved on	05-01-2024

Version – 2.0

[30 DECEMBER 2023]

PolicyStatement

- 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 suchresources.

- AccesstoCompany'ssystemsmustberestrictedtoonlyauthorizedusersorprocesses,basedon the principle of strict need to know and leastprivilege.

Background

- Access controls are necessary to ensure only authorized users can obtain access to theCompany's information andsystems.

- Accesscontrolsmanagetheadmittanceofuserstosystemandnetworkresourcesbygranting users access only to the specific resources they require to complete their job-relatedduties.

Policy Objective

- TheobjectiveofthispolicyistoensuretheInstitutionhasadequatecontrolstorestrictaccess to systems anddata.

Scope

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

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 andapplications.

- "System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems andapplications.

- "PrivilegedAccounts"aresystemorapplicationaccountsthathaveadvancedpermissions (as comparedtoregularuseraccountpermissions)onsuchsystemsorapplications.Examplesof user accounts with privileges include: administrative and super useraccounts.

- "Access Privileges" are systems permissions associated with an account, including permissionstoaccessorchangedata,toprocesstransactions,createorchangesettings,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 networkservice.

- "Nominative User Accounts" are user accounts that are named after aperson.

- "Non-disclosureAgreement"isacontractbetweenapersonandtheCompanystatingthatthe 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 (includingnetworks, systems, applications, computers and mobile devices) based on the followingprinciples:
  - ➢ **Need to know** – users or resources will be granted access to systems thatare necessary to fulfill their roles andresponsibilities.
  - ➢ **Least privilege** – users or resources will be provided with the minimumprivileges necessary to fulfill their roles andresponsibilities.
- Requests for users' accounts and access privileges must be formally documentedand appropriatelyapproved.
- 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 systemowner.
- Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administratorsor application developers only.
- Where possible, the Company will set user accounts to automatically expire at a pre-setdate. Morespecifically,
  - ➢ Whentemporaryaccessisrequired,suchaccesswillberemovedimmediatelyafterthe user has completed the task for which the access wasgranted.
  - ➢ User accounts assigned to contractors will be set to expire according to the contract's expirydate.
  - ➢ User accounts will be disabled after 3 months of inactivity. This does not apply to accounts assigned toemployees.
  - ➢ 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 orceases to have a legitimate reason to access Company'ssystems.
- 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 privilegesinclude:
  - ➢ An active account assigned to external contractors, vendors or employees that no longer work for theCompany.
  - ➢ Anactiveaccountwithaccessrightsforwhichtheuser'sroleandresponsibilitiesdonot require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within afinancial 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 activeaccounts.
- All access requests for system and application accounts and permissions will bedocumented using the ticketing

system inplace.

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 appropriatelyapproved.

Guiding Principles – Shared User Accounts

- Wherepossible,theuseofspecificnetworkdomain"securitygroups"shouldbeusedtoshare common access permissions across many users, instead of sharedaccounts.
- Shareduseraccountsareonlytobeusedonanexceptionbasiswiththeappropriateapproval. This includes general user accounts such as "guest" and "functional"accounts.
- When shared accounts arerequired:
  - ➤ Passwords will be stored and handled in accordance with the PasswordPolicy.
  - ➤ 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 andrestricted.

Vendor or Default User Accounts

- Wherepossible,alldefaultuseraccountswillbedisabledorchanged.Theseaccountsinclude "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-theshelf" systems andapplications.

Test Accounts

- Testaccountscanonlybecreatediftheyarejustifiedbytherelevantbusinessareaorproject teamandapprovedbytheapplicationowner,throughaformalrequesttotheITDirectororthe 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 approvedappropriately.
- Test accounts will be disabled / deleted when they are no longernecessary.

Contractors and Vendors

- In accordance with the Contract Management Policy, contracts with contractors / vendors will includespecificrequirementsfortheprotectionofdata.Inaddition,contractor/vendorrepresentatives will be required to sign a Non-disclosure Agreement ("NDA") prior to obtaining approval to access Institution systems and applications.
  - ➤ Priortograntingaccessrightstoacontractor/vendor,theITDirectororHelpDeskmustverify the requirements of Section 11.1 have been compliedwith.
  - ➤ Thenameofthecontractor/vendorrepresentativemustbecommunicatedtotheITHelpDesk at least 2 business days

before the person needsaccess.

- The Company will maintain a current list of external contractors or vendors having access to Company'ssystems.
- Theneedtoterminatetheaccessprivilegesofthecontractor/vendormustbecommunicated to the IT Help Desk at least 1 business day before the contractor / vendor representative's need for such access ends.

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 PasswordPolicy.
- Alternative authentication mechanisms that do not rely on a unique ID and password mustbe formallyapproved.
  - ➢ Remote access to Company's systems and applications must use two-factor authenticationwhere possible.
  - ➢ System and application sessions must automatically lock after 15 minutes ofinactivity.

Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Board of Director	• Approve and formally support thispolicy.
President, Administration	• Review and formally support thispolicy.
IT Director/Designated officer	• Develop and maintain thispolicy. • Review and approve any exceptions to the requirements of thispolicy. • Take proactive steps to reinforce compliance of all stakeholders with thispolicy.
Supervisors or Company's Representative	• Support all employees and others in the understanding of the requirementsof thispolicy. • Immediately assess and report to the IT service desk anynon-compliance instance with thispolicy.
Contract Administrators	• Ensure that the responsibilities and security obligations of each party tothe contractual relationship are outlined in the contract executed between the Company's and thecontractor/sub-contractor.
Human Resources	• Present each new employee or contractor with the relevant Company's IT andSecurity Policies, upon the first day of commencing work withCompany's. • Support all employees and other in the understanding of the requirementsof thispolicy.
All users (Employees and contractors, Visitors and or Volunteers)	• Report all non-compliance instances with this policy (observed or suspected)to their Supervisor, Instructor or Company's Representative as soon aspossible.

Exceptions to the Policy

- Exceptions to the guiding principles in this policy must be documented and formallyapproved by the ITDirector/Designated Officer.

- **Policy exceptions must describe:**
  - ➢ The nature of theexception
  - ➢ A reasonable explanation for why the policy exception isrequired
  - ➢ Any risks created by the policyexception
  - ➢ Evidence of approval by the ITDirector
- **Inquiries**
  - ➢ Inquiries regarding this policy can be directed to the ITDirector/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 M/s. ANJANEY STOCK BROKING LIMITED

Mr. Pramod Kumar Sanganeria
(Designated Officer)
Date: 05-01-2024