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

PASSWORD POLICY

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]

Purpose:

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

Scope:

The scope of this policy includes all end-users and personnelwho have or are responsible for an account (or any form of access thatsupports or requires a password) on any system/service in the NICdomain.Theseincludepersonnelwiththeirdesignateddesktopsystems. The scope also includes designers and developers of individualapplications.

Policy:

PolicyStatements

- ✓ Forusers havingaccountsforaccessingsystems/services
- ✓ Users shall be responsible for all activity performed withtheir personal user IDs. Users shall not permit others toperform any activity with their user IDs or perform anyactivitywith IDsbelonging tootherusers.
- ✓ Alluser-levelpasswords(e.g.,email,web,desktopcomputer, etc.) shall be changed periodically (at leastonce every three months). Users shall not be able toreuseprevious passwords.
- ✓ Password shall be enforced to be of a minimum lengthandcomprisingofmixofalphabets,numbersandcharacters.
- ✓ Passwords shall not be stored in readable form in batchfiles,automaticlogonscripts,Internetbrowsersorrelateddatacommunicationsoftware,incomputerswithout access control, or in any other location whereunauthorizedpersonsmightdiscoverorusethem.
- ✓ All access codes including user ID passwords, networkpasswords, PINs etc. shall not be shared with anyone,including personal assistants or secretaries. These shallbetreatedassensitive,confidentialinformation.
- ✓ AllPINs(PersonalIdentificationNumbers)shallbeconstructedwiththesamerulesthatapplytofixedpasswords.
- ✓ Passwordsmustnotbecommunicatedthoughemailmessages or other forms of electronic communicationsuchasphoneto anyone.
- ✓ Passwords shall not be revealed on questionnaires orsecurityforms.
- ✓ Passwords of personal accounts should not be revealedto the controlling officer or any co-worker even while onvacationunlesspermittedtodosobydesignatedauthority.
- ✓ The same password shall not be used for each of thesystems/applications to which a user has been grantedaccesse.g.aseparatepasswordtobeusedforaWindowsaccountandanUNIXaccountshouldbeselected.
- ✓ The "Remember Password" feature of applications shallnotbe used.
- ✓ Users shall refuse all offers by software to place a cookieon their computer such that they can automatically logonthenexttimethattheyvisitaparticularInternetsite.
- ✓ First time login to systems/services with administratorcreatedpasswords,shouldforcechangingofpasswordbythe user.
- ✓ If the password is shared with support personnel forresolving problems relating to any service, it shall bechangedimmediatelyafter thesupport session.
- ✓ Thepasswordshallbechangedimmediatelyifthepassword is suspected of being disclosed, or known tohavebeendisclosedtoanunauthorizedparty.

- ✓ Fordesigners/developersofapplications/sites
- ✓ No password shall be traveling in clear text; the hashedform of the password should be used. To get around thepossibility of replay of the hashed password, it shall beusedalongwitharandomizationparameter.
- ✓ The backend database shall store hash of the individualpasswordsandneverpasswordsinreadableform.
- ✓ Password shall be enforced to be of a minimum lengthandcomprisingofmixofalphabets,numbersandcharacters.
- ✓ Usersshallberequiredtochangetheirpasswordsperiodicallyandnotbeabletoreusepreviouspasswords.
- ✓ For Password Change Control, both the old and newpasswordsarerequiredtobegivenwheneverapasswordchangeisrequired.

Policy for constructing a password:

Alluser-levelandsystem-level passwords must conform to the following generalguidelinesdescribed below.

- ✓ Thepasswordshallcontainmorethaneightcharacters.
- ✓ Thepasswordshallnotbeawordfoundinadictionary(Englishorforeign).
- ✓ Thepassword shallnotbe aderivative oftheuserID,e.g. <username>123.
- ✓ Thepasswordshallnotbeaslang,dialect,jargonetc.
- ✓ The password shall not be a common usage words such asnamesoffamily,pets,friends,co-workers,fantasycharacters,etc.
- ✓ The password shall not be based on computer terms andnames,commands,sites,companies,hardware,software.
- ✓ The password shall not be based on birthdays and otherpersonalinformationsuchasaddressesandphonenumbers.
- ✓ The password shall not be a word or number pattern likeaaabbb, qwerty, zyxwvuts, 123321, etc. or any of theabovespelledbackwards.
- ✓ The password shall not be any of the above preceded orfollowedbyadigit (e.g., secret1,1secret).
- ✓ The password shall be a combination of upper- and lower-casecharacters(e.g.a-z,A-Z),digits(e.g.0-9)andpunctuationcharactersaswellandothercharacters(e.g., @#$%^&*() _+|~-=\` {} []:";'<>? /).
- ✓ Passwords shall not be such that they combine a set ofcharactersthatdonotchangewithasetofcharactersthatpredictably change.

Suggestions for choosing passwords:

- ✓ Passwordsmaybechosensuchthattheyaredifficult-to-guessyeteasy-to-remember.Methodssuch asthefollowing maybeemployed:
- ✓ String together several words to form a pass-phrase as apassword.
- ✓ Transformaregularwordaccordingtoaspecificmethode.g. making every other letter a number reflecting itspositionin the word.
- ✓ Combinepunctuationand/ornumberswitharegularword.
- ✓ Createacronymsfromwordsinasong,apoem,oranyotherknown sequence ofwords.
- ✓ Bumpcharactersinawordacertainnumberoflettersupordown the alphabet
- ✓ Shiftawordup,down,leftorrightonerowonthekeyboard.

Responsibilities:

- ✓ Allindividualusershavingaccountsforaccessingsystems/servicesintheNICdomain,andsystem/networkadministr

ators of NIC servers'/ network equipment shall ensuretheimplementationofthispolicy.

✓ Alldesigners/developersresponsibleforsite/applicationdevelopment shall ensure the incorporation of this policy in theauthentication modules, registration modules, password changemodulesoranyothersimilarmodulesintheirapplications.

<u>Compliance</u>

✓ Personnel authorized as Internal Audit shall periodically reviewtheadequacyofsuchcontrolsand theircompliance.

✓ Personnel authorized as Application Audit shall check respectiveapplicationsforpasswordcomplexityandpasswordpolicyincorporation.

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