Jan Parichay

(Single Sign-On)

Password Policy

Submitted by

National Informatics Centre

4th Floor, Block III, Delhi IT
Park, Shastri Park

New Delhi 110053

Website: www.nic.in

DOCUMENT CONTROL

DOCUMENT NAME: JanParichay Password Policy

DOCUMENT ID REFERENCE:

AUTHORIZATION:

Prepared By	Reviewed By	Reviewed By	Authorized By
Name: Ankit Gochhayat	Name: Prashant Sharma	Name: Amit Kumar	Name: Anil Kumar Jha
Designation: PMU	Designation: Java Team Lead	Designation: Scientist D	Designation: Scientist F

SECURITY CLASSIFICATION: Restricted

VERSION HISTORY:

Issue Date	Effective Date	Description
01.03.2024	01.03.2024	V1.0

DISTRIBUTION LIST:

The following persons hold the copies of the documents; all amendments and updates to the the document must be distributed to the distribution list.

S.N.	Name	Location	Document type
1	Amit Kumar	NIC, New Delhi	Soft copy, Hardcopy
2	Seema Khanna	NIC, New Delhi	Soft copy, Hardcopy

CONFIDENTIAL:

This document contains restricted information about the National Informatics Centre. The access level for the document is specified above. The addressee should honor this access right by preventing intentional or accidental access outside the access scope.

DISCLAIMER:

This document is solely for the information of National Informatics Centre and should not be used, circulated, quoted or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.

1. 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.

2. Scope

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the NIC domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

3. Policy

3.1 For users having accounts for accessing systems/services

- All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords.
- Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.
- Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.
- Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.
- Passwords shall not be revealed on questionnaires or security forms.
- Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.
- The "Remember Password" feature of applications shall not be used.
- If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.
- The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

3.2 Policy for constructing a password

All user-level and system-level passwords must conform to the following general guidelines described below:

- The password shall contain more than eight characters.
- The password shall not be a word found in a dictionary (English or foreign).
- The password shall not be a derivative of the user ID, e.g. 123.
- The password shall not be a slang, dialect, jargon etc.
- The password shall not be a “common usage word” such as names of family, pets, friends, co-workers, fantasy characters, etc.
- The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.

- The password shall not be based on birthdays and other personal information such as addresses and phone numbers.
- The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.
- The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., !@# $%^&*()_+|~-=\`{}[]:";'<>?,./).
- Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

3.3 Suggestions for choosing passwords

Passwords may be chosen such that they are difficult-to-guess yet easy-to remember. Methods such as the following may be employed:

- String together several words to form a passphrase as a password.
- Transform a regular word according to a specific method e.g., making every other letter a number reflecting its position in the word.
- Combine punctuation and/or numbers with a regular word.
- Create acronyms from words in a song, a poem, or any other known sequence of words.
- Bump characters in a word a certain number of letters up or down the alphabet.
- Shift a word up, down, left or right one row on the keyboard.’