Password Policy

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 Policy Statements

3.1.1 For users having accounts for accessing systems/services

3.1.1.1 Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.

3.1.1.2 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.

3.1.1.3 Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.

3.1.1.4 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.

3.1.1.5 All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.

3.1.1.6 All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.

3.1.1.7 Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.

3.1.1.8 Passwords shall not be revealed on questionnaires or security forms.

3.1.1.9 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.

3.1.1.10 The same password shall not be used for each of the systems/applications to which a user has been granted access e.g. a separate password to be used for a Windows account and an UNIX account should be selected.

3.1.1.11 The "Remember Password" feature of applications shall not be used.

3.1.1.12 Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

3.1.1.13 First time login to systems/services with administrator created passwords, should force changing of password by the user.

3.1.1.14 If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

3.1.1.15 The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

3.1.2 For designers/developers of applications/sites

3.1.2.1 No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter.

3.1.2.2 The backend database shall store hash of the individual passwords and never passwords in readable form.

3.1.2.3 Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.

3.1.2.4 Users shall be required to change their passwords periodically and not be able to reuse previous passwords.

3.1.2.5 For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

3.2 Policy for constructing a password: All user-level and system-level passwords must conform to the following general guidelines described below.

3.2.1 The password shall contain more than eight characters.

3.2.2 The password shall not be a word found in a dictionary (English or foreign).

3.2.3 The password shall not be a derivative of the user ID, e.g. <username>123.

3.2.4 The password shall not be a slang, dialect, jargon etc.

3.2.5 The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.

3.2.6 The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.

3.2.7 The password shall not be based on birthdays and other personal information such as addresses and phone numbers.

3.2.8 The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.

3.2.9 The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).

3.2.10 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., !@# $%^&*()_+|~-=\`{}[]:";'<>?,./).

3.2.11 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:

3.3.1 String together several words to form a pass-phrase as a password.

3.3.2 Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.

3.3.3 Combine punctuation and/or numbers with a regular word.

3.3.4 Create acronyms from words in a song, a poem, or any other known sequence of words.

3.3.5 Bump characters in a word a certain number of letters up or down the alphabet.

3.3.6 Shift a word up, down, left or right one row on the keyboard.

4. Responsibilities:

4.1 All individual users having accounts for accessing systems/services in the NIC domain, and system/network administrators of NIC servers/ network equipments shall ensure the implementation of this policy.

4.2 All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

5. Compliance

5.1 Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance.

5.2 Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.