North Shore Technologies

Password Policy

Version History:

Ver.	Date	Description of Change	Authored / Revised By	Reviewed By	Approved By
1.0	11th June, 2012	Draft	Ajeet	Saket	
1.1	10th July, 2012	Initial Version	Ajeet	Saket	GM Dua
2.0	30th Oct 2013	Update section 5.0	Ajeet	Saket	GM Dua
2.1	10th March 2014	Update section 4.0	Ajeet	Saket	Ajay Kumar Zalpuri
2.2	29th July 2015	Update section 4.0 for Password string definition & default password setting for new joining	Ajeet	Saket	Ajay Kumar Zalpuri
2.3	27th May 2017	Update section 5.0 for IT admin password	Ajeet	Saket	Ajay Kumar Zalpuri
2.4	5th Feb 2018	Update section 3.0 for Multifactor Authentication applied for email users	Ajeet	Saket	Ajay Kumar Zalpuri
2.5	17th May 2019	Update section 6 for Keeping your password safe and add point number f, g, h, j	Ajeet/ Rahul Raj	Saket	Ajay Kumar Zalpuri

1.0 Overview

Most users log on to their local computer and to remote computers by using a combination of their username and a password typed at the keyboard. Although alternative technologies for authentication, such as biometrics, smartcards, and one-time passwords, are available for all popular operating systems, most organizations still rely on traditional passwords and will continue to do so for years to come. Therefore, it is very important that organizations define and enforce password policies for their computers that include mandating the use of strong passwords. Strong passwords meet several requirements for complexity - including length and character categories - that make passwords more difficult for attackers to determine. Establishing strong password policies for your organization can help prevent attackers from impersonating users and can thereby help prevent the loss, exposure, or corruption of sensitive information.

2.0 Purpose

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

3.0 Scope

This policy applies to all computers that are connected to the NST network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally owned computers attached to the NST network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

4.0 General Policy:

- Configure password policy settings in an Active Directory Domain.
- Configure password policy settings on stand-alone computers.

  - **Multi factor authentication** has been enabled for all O365 users.

    User required OTP every login on web access and once for their desktop setup

  - **Enforce password history** determines the number of unique new passwords a user must use before an old password can be reused. The value set for these 2 cycles for password set.
  - **Default Password** for new joining e.g. Ram Kumar Singh, password will be RaSisvam123

- **Maximum password age** determines how many days a password can be used before the user is required to change it. Set this value to 90 days.
- **Passwords must meet complexity requirements** determine whether password complexity is enforced. If this setting is enabled, user passwords meet the following requirements:

  - *Not contain the user's account name or parts of the user's full name that exceed two consecutive characters*
  - *Be at least eight characters in length*
  - *Contain characters from three of the following four categories:*
    - *English uppercase characters (A through Z)*
    - *English lowercase characters (a through z)*
    - *Base 10 digits (0 through 9)*
  - *Non-alphabetic characters (for example, $, #, %)*

- Complexity requirements are enforced when passwords are changed or created.
- After leaving the Organization the email id of the user will be deactivated immediately (24 hrs.). Wherever for business reason the deactivation is not possible, his/her password will be changed immediately (24 hrs.) with the approval of Business unit head. In such cases the deactivation of email id should be done maximum within a period of 90 days.

5.0 IT System Department Responsibilities

The following activities are the responsibility of the NST system department:

1. The IT System department is responsible for maintaining and updating this Password. Policy.

2. The IT System department the vendor site as will keep the Password policy automatically updated by network administrator.

3. The IT System department shall be responsible for checking and facilitating all NST owned and installed desktop workstations, laptops, and servers.

4. The IT System department shall be responsible for maintain admin password in a list provide this information in sealed envelope to Managing Director or Business Head for business continuity in case of any disaster.

6.0 Department and Individual Responsibilities:

The following activities are the responsibility of NST departments and employees:

1. Departments must ensure that all departmentally managed computers have password policy enabled that is in keeping with the standards set out in this policy.

2. Departments that allow employees to use personally owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

3. All employees are responsible for maintaining Password change practice

4. **Keeping your password safe:** To protect the information in your computer account from unauthorized access:

    a. Do not share your username and password with anyone. Except in the case of a shared departmental account, you should never disclose the passwords for your computer accounts to anyone. If you receive a phone call or an email message requesting such information, please report the incident to the IT Service Desk. Remember, no one from IT services will ever ask for your password.

    b. If shared in any circumstances, please change immediately after the work finished.

    c. Do not write down your password and store them anywhere in your office

    d. Remember to log off. Do not leave a PC without logging off. Check that you are logged off before you leave the PC.

    e. Do not download programs from unknown sources on the internet some of the free software available on the internet may contain viruses, and some can allow unauthorized users to gain access to your account without your knowledge.

    f. Do not talk about a password in front of others

    g. Do not reveal a password on questionnaires or security forms

    h. Do not share a password with family members

    i. Do not reveal a password to a co-worker while on vacation

    j. Do not let anyone see you type your password

7.0 Enforcement:

This policy shall be implemented, administered, and enforced by the System Administrator.