



Password Policy




October 2022

DOCUMENT HISTORY AND SIGN OFF

DOCUMENT HISTORY

Document Title	Password Policy
Document Reference Number	NSP/EVCIT/2022/126
Initiating Department	Information Technology
Date Created	September 2022
Document Version	Version 1
Effective Date	October 2022
Date of Next Review	October 2024

SIGN OFF AND APPROVAL

S/N	AUTHORIZING OFFICERS ROLE	JOB TITLE	NAME	SIGNATURE	DATE
1	Created By	Head, Information Technology	EMMANUEL ABIMBOLA OLOWOOKERE		07-12-22
2	Reviewed By	Chief Internal Audit & Risk Management Officer	IKECHUKWU OKOLI		07 - 12 - 22
3	Approved By	EVC/CEO	OLUBUNMI PETERS		07-12-22

This sign-off authorizes the immediate implementation of this document.

1.0 SCOPE

Primarily covers Microsoft 365, but most advice is applicable to IT systems connected to North South Power Company Limited's (NSPCL) networks.

2.0 POLICY

This document gives an outline of the password policy for North South Power. It will cover creating good passwords, multi-factor authentication, and password management. While the recommendations concern Microsoft 365, it is strongly advised that the recommendations are followed for personal accounts. This will help keep them secure.

Passwords currently expire 100 days after they have been set.

The minimum length of the password is 8 characters. The maximum is 256 characters. The password needs to have at least 3 of the following combinations:

- Lowercase characters
- Uppercase characters
- Numbers
- Symbols

Users are recommended to use a unique to password for each account they have. Reusing passwords leaves other accounts using the same password vulnerable, if one account is hacked. In addition, users should never create a password such as Password1 or P@ssword. These are extremely easy to guess.

Users should consider using a passphrase, such as a sentence. Users can interpolate symbols and numbers into the sentence, as they see fit. Pass-phrases have the advantage of being both long, and easy to remember. Alternatively, using 4 or 5 words picked at random from a dictionary, and replacing some characters with symbols and uppercase letters is another viable alternative.

Users are advised to never share their passwords with other people. Sharing your password gives someone else access to your account and leaves you vulnerable to attacks on the other person.

2.1 Remembering passwords

You can make use of a password manager to keep track of your passwords. Password managers can also be used to automatically create secure passwords, using criteria defined by the user. You can use the password manager on Microsoft Authenticator for this task.

For more options, you can ask any member of IT staff to recommend you a password manager.

2.2 Multi-factor Authentication

Multi-factor authentication means you require more than 1 way to sign-in to your account, in this case your phone and PC. It is important that you keep the phone number associated with your account up to date.

When using multi-factor authentication, you have 3 means of authenticating using your phone. You can receive a call, text message or use your Microsoft Authenticator app.

2.3 Changing your default authentication method

- Sign in to office.com
- Click on the icon that has your initials in the top right
- Select view account
- On the task bar on the left, select Security info
- You can use add method to add a new means of authentication if you wish
- Select Change, and use the drop down to switch to the method you want

2.4 Setting up your Authenticator app

- Open your App store (Play Store or Apple App Store)
- Search for Microsoft Authenticator
- Download the application, and open it
- Follow the instructions for setting up your phone

For more options, if you require any assistance concerning Password and/or Password Security, kindly consult with any member of IT Staff.