NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Overview

This document accompanies the NTPC cybersecurity Baseline Control 5.3 – Password Policy Length and Reuse. The intention of this document is to help NTPC employees and contractors create passwords that satisfy our cybersecurity requirements while balancing the ease of remembering your password.

NTPC's password philosophy has shifted. Previously the recommendation was to use a shorter password (at least 8 characters) and use character substitution to make it more complex with the consideration that the password would be harder to hack, fully acknowledging that it would be harder to memorize.

As cybersecurity tools to crack passwords have matured, the bar to be able to crack passwords has become very low. In general today the complexity of a password is measured by its entropy. Entropy is a measure of how un-guessable a password is. For example, the password "123456" and "qwerty" were two of the top passwords used in 2022. These are examples of very low entropy passwords.

By way of example, a very high entropy password example is "calcium#P@JAMAS". This password though may be difficult to remember. Another high entropy password example is "correct horse battery staple". The second example is reasonably easy to remember. Entropy is measured in bits. [1]The first example has 93 bits of entropy, and the second example has 131 bits of entropy.

To support increasing entropy in passwords, NTPC has defined two password standards that balance requirements of setting a password against the ease of remembering that password. In support of this, there are now two password standards, a default, and an opt-in password standard.

[1] See for yourself how much entropy your password has: https://timcutting.co.uk/tools/password-entropy

NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Changes as of March 2023

The old password standard contained the following password requirements:

- Must be 8 or more characters long, and is valid for 90 days
- Cannot re-use the last 24 passwords
- Password must be made up of 3 of the 4 following sets of characters
    - Lowercase letters (a-z)
    - Uppercase letters (A-Z)
    - Numbers (0-9)
    - Special Characters (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

New Default Password Standard (referred to as the **NTPC 90-Day Password**)

- Must be **12** or more characters long, and is valid for 90 days
- Cannot re-use the last **40** passwords
- Password must be made up of 3 of the 4 following sets of characters
    - Lowercase letters (a-z)
    - Uppercase letters (A-Z)
    - Numbers (0-9)
    - Special Characters (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
- **Must pass the Microsoft Azure Password Protection Service**

New Opt-In Password Standard (referred to as the **NTPC 360-Day Password**)

- Must be **20** or more characters long, and is valid for 360 days
- Cannot re-use the last **10** passwords
- **There are no complexity requirements**
- **Must pass the Microsoft Azure Password Protection Service**

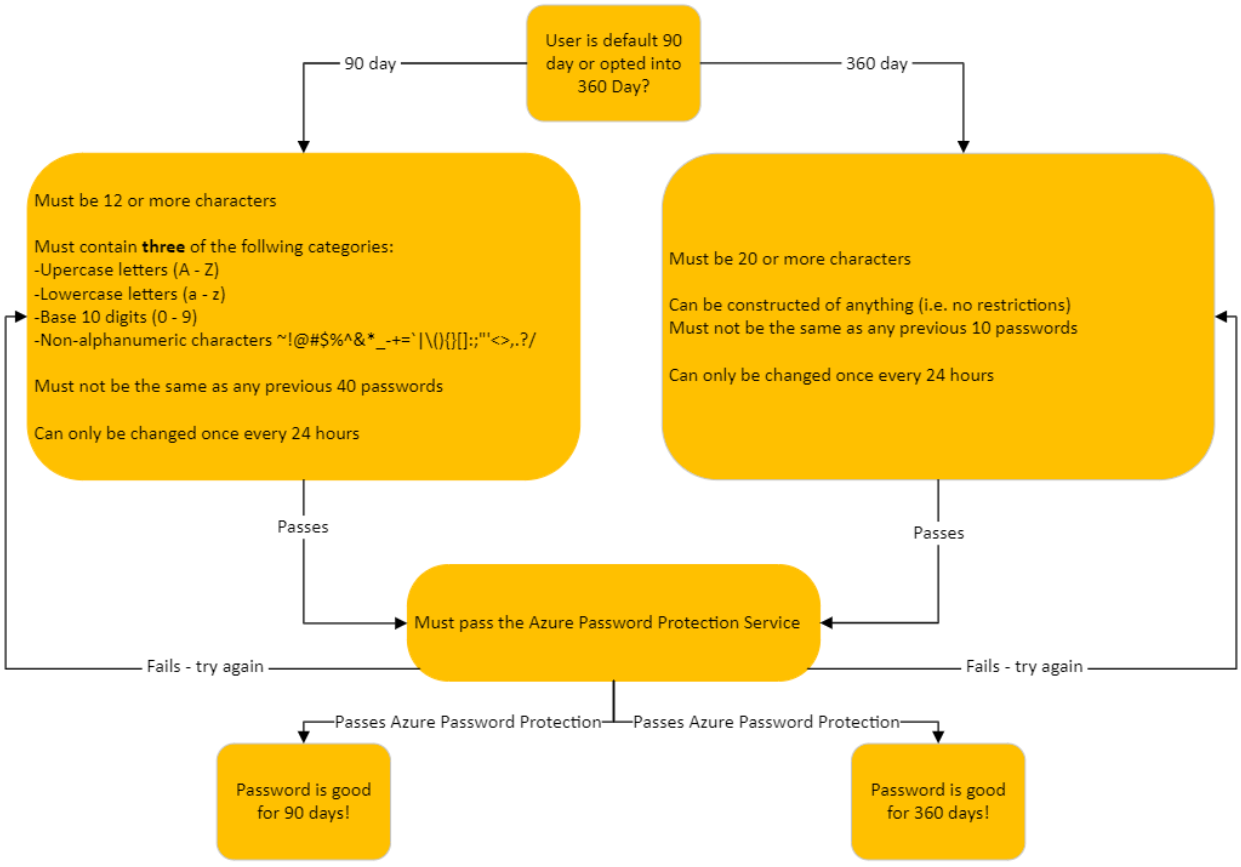
NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Password Creation Procedure

NTPC has implemented a two-tier password policy which seeks to give its employees and contractors flexibility in creating easy to remember passwords based upon user preference. Employees and contractors by default will be enforced to set a minimum 12-character password which will expire every 90 days. If an employee or contractor opts-in (at anytime), they can choose to be forced to use a 20-character password which will only expire every 360 days. The details are as follows.

Valid password construction consists of the following logic flow:



NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Azure Password Protection Service details

NTPC has implemented the Microsoft Azure Active Directory Password Protection service. This tool aims to prevent users from using common passwords that hackers use to compromise accounts. This service blocks known weak passwords and their variants, and other common terms specific to NTPC. It also includes custom banned password lists and self-service password reset capabilities.

Evaluation of a password is based upon a score that must total five (5) or more points if it contains a banned password. The following are steps that execute to evaluate and grade a password.

Step 1: Normalization

A new password first goes through a normalization process. This technique allows for a small set of banned passwords to be mapped to a much larger set of potentially weak passwords.

Normalization has two parts:

- All uppercase letters are changed to lower case.
- Then, common character substitutions are performed, such as in the following example:

Original character	Substituted letter
0	o
1	l
$	s
@	a
9	g

Consider the following example:

- The password “abbreviation” is in the global list of banned passwords.
- A user tries to change their password to “Abbrev!ation”.
    - The user has the default setting for 90-day passwords, this password would be accepted for 90-day requirements and is then passed off to be evaluated against the Azure Password Protection service
- Even though “Abbrev!ation” isn’t banned, the normalization process converts this password to “abbreviation”.

NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Step 2: Check if the password is considered banned

A normalized password is then examined using additional matching behavior and a score is generated. The final score determines if the password change request is accepted or rejected only if it contains a banned password.

Fuzzy matching behavior on banned passwords

Fuzzy matching is used on the normalized password to identify if it contains a password found on either the global or the custom banned password lists. The matching process is based on an edit distance of one (1) comparison.

Consider the following example:

- The password “abcdef” is banned
- A user tries to enter the password to one of the following:
  - ‘abcdeg’ – note that the last character changed from an ‘f’ to a ‘g’
  - ‘abcdefg’ – note that the ‘g’ is added to the end
  - ‘abcde’ – note that the trailing ‘f’ was deleted from the end
- Each of the above passwords doesn’t specifically match the banned password “abcdef”
  - However, since each example is within an edit distance of 1 from the banned password “abcdef”, they are all considered as a match to “abcdef”
- All three of the password examples would be marked as a banned password.

Substring matching (on specific terms)

Substring matching is used on the normalized password to check for the user's first and last name as well as the tenant name. Tenant names are “ntpc”, “ntenergy” and “nwtpowercorporation”. Substring matching is only enforced on names and other terms that are at least four characters long.

Consider the following example:

- A user named Poll tries to change their password to “p0LL23fb”.
- After normalization, this password would become “poll23fb”.
- Substring matching finds that the password contains the user’s first name “Poll”.
- Even though “poll23fb” wasn’t specifically on either the banned password list, substring matching found “Poll” in the password.

NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Score Calculation

The next step is to identify all instances of banned passwords in the user's normalized new password after fuzzy and substring searches. Points are assigned based on the following criteria:

1. Each banned password that's found in a user's password is given one (+1) point.
2. Each remaining character that is not part of a banned password is given plus one (+1) point.
3. A password must be at least five (5) points to be accepted.

Note that #1 above is not a typo, the logic is that "even if a user's password contains a banned password, the password may still be accepted if the overall password is strong enough otherwise".

Consider the following examples:

Example 1:
Assume that "NTPC" and "blank" are in the banned password lists. A user tries to change their password to "N7PCBlank12":

- After normalization, this password becomes "ntpcblank12"
- The matching process finds the password contains two banned passwords: "ntpc" and "blank".
- This password is then given the following score:
  - [ntpc] = +1
  - [blank] = +1
  - [1] = +1
  - [2] = +1
  - Total = 4
- This password would be rejected because it does not add up to five (5) or more.

Example 2:
Assume that NTPC and "blank" are in the banned password lists. A user tries to change their password to "N7PCBl@nkf9!":

- After normalization, this password becomes "ntpcblankf9!"
- The matching process finds the password contains two banned passwords: "ntpc" and "blank".
- This password is then given the following score:
  - [ntpc] = +1

NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

    - [blank] = +1
    - [f] = +1
    - [9] = +1
    - [!] = +1
    - Total = 5
- This password would be accepted because it is at least five (5) points.

Example 3:
Assume that the employee setting this password has opted into the 20 Character password. NTPC and “blank” are in the banned password global lists. A user tries to change their password to “my eye hook hurts now”:

- Note that because this is a 20 Character opt-in password, there are no complexity requirements on the composition of the characters.
- After normalization, this password becomes “myeyehookhurtsnow”
- The fuzzy and substring matching process does not find any banned words.
- No further evaluation of the password occurs, and it is accepted.

Example 4:
Assume that the employee setting this password has opted into the 20 Character password. NTPC is in the banned password global lists. A user tries to change their password to “ntpcntpcntpcntpcnptc”:

- Note that because this is a 20 Character opt-in password, there are no complexity requirements on the composition of the characters.
- After normalization, this password becomes “ntpcntpcntpcntpcnptc”
- The matching process finds the banned password “ntpc”
- No further evaluation of the password occurs, and it is accepted.
- This password is then given the following score:
    - [ntpc] = +1
    - [ntpc] = +1
    - [ntpc] = +1
    - [ntpc] = +1
    - [ntpc] = +1
    - Total = 5
- The logic behind this is that the overall entropy (complexity) of this password is greater than the individual component banned password – this is called “5 wrongs make a right”.
    - Note that this example and several others have been explicitly banned.

NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Frequently Asked Questions

How do I opt-in to the 360-day password?

- Email helpdesk@ntpc.com and indicate you would like to opt-in to the 360-day password. The helpdesk will respond that you are now enabled, which takes effect immediately, but won't be applied until the next time you have to change your password (or choose to do it sooner)

Are there really no requirements on the 360-day password?

- That's correct, literally any combination of anything you can type in the password field will be accepted (if it also passes the Azure Password Protection Service)

How do I change my password?

There are two primary ways:

1. Signed onto any PC at NTPC, you can press Control+Alt+Delete and then select "Change a Password".
2. Using any modern web browser go to https://office.com/signin and select settings from the upper right-hand corner (it looks like a gear icon). Choose "Change your password".

I keep entering a new password that meets the 90 or 360-day password requirements, but I'm getting a message that says something like "*Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.*"

- Chances are you are bumping into a banned password from the Azure Password Protection Service. Unfortunately, the error message is not particularly clear. You can either try a different password, or email the helpdesk@ntpc.com who can tell you more precisely why the error message is being presented. Please don't share with the IT Division employee the password you were trying to use, they don't need it to diagnose why its not working.

Can you tell me all the banned passwords in the Azure Password Protection Service?

- The short answer is no.
- Microsoft does not reveal which passwords are in their global list of banned passwords.
- NTPC maintains its own list of banned passwords, these are not secret, but we won't list them electronically for you. Feel free to touch base with any IT Division employee either in person or on the phone if you would like to know more.

NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Why is the 90-day password easier to guess than the 360-day password?

- This isn't necessarily the case. NTPC is trying to encourage our staff and contractors to create easier to remember passwords so they don't have to be written down. Our logic is:
    - The 90-day password can be shorter, but you have to make it more complex to increase entropy. Because it's shorter, it will potentially be easier to hack. A well-formed complex 90-day password will be as secure as a 360-day password, but it will be harder to remember.
    - The 360-day password, by sheer length, is dramatically harder to hack. Even the simplest 360-day password will be harder to hack than the 90-day password that minimally meets those requirements.
    - We are hoping many staff opt-into the 360-day password because:
        - They can be easier to remember.
        - They are good for practically a year.

I heard something about 5 wrongs make a right, what's the deal with that?

- Take for example the password "password". This password is banned by the Azure Password Protection Service.
- However, if you create your password as "passwordpasswordpasswordpasswordpassword" the overall password has massive entropy. So although "password" is banned, technically password five times would be permitted in the 360-day password.
    - That being said, this is in the NTPC custom list of banned passwords!

Will you teach me how to hack passwords?

- Yes! But only your own. The more knowledge you have around how passwords work to secure systems, the more likely you are to create a more secure password, and we would be pleased to help you on that journey.

Now that I have a really strong password, will I still have to Two-Factor Authenticate?

- In the next 2-3 years, yes. NTPC is moving from something called "Medium Assurance Authentication" to "High Assurance Authentication". Until we can move to the High Assurance Authentication, you will still need to provide a second factor for authentication.
- The holdup is that all applications need to support High Assurance Authentication, and many of NTPC's systems do no yet support this, or need to be reconfigured to support this. This reconfiguration or replacement will take 2-3 years to complete.

NORTHWEST TERRITORIES POWER CORPORATION

4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

I heard something about NTPC "going passwordless"?

- No one likes passwords, not the least of which are Information Technology workers that are charged with securing systems with a combination of usernames and passwords.
- Passwordless authentication allows a user to log into a computer system without providing a password or any knowledge-based secret. In most setups this means telling the computer system your publicly known user identifier (a username, an email address, etc), and then completing the authentication process by providing secure proof of identity through a registered device or token.
- This can be thought of as a really secure way of Two-Factor Authentication, and is the outcome of getting to High Assurance Authentication
- NTPC has already enabled High Assurance Authentication, but not all NTPC systems support it. Examples of systems that do not require a password to sign on if you have registered either a biometric token (face scan, fingerprint), or the Microsoft Authenticator with Phone Sign In:
    - Your work computer – if it has a face scanning capable camera or fingerprint scanner that you have chosen to opt-in
    - Microsoft 365 cloud services (all of the online applications)
- Systems that NTPC is currently working on to become passwordless:
    - Penny (timesheets)
    - K2 Forms
    - WorkPlace

What is SSO (single sign-on)?

- This is a technology that passes through your authentication from one system to another. For example, if you sign onto your work computer using a passwordless option, if an application installed on your computer has been configured for SSO you won't be prompted to sign in a second time to that application. The logic is that you have already proven who you are once, you can have the application ask to see if that already occurred.

Why 360 days and not 365 days?

- Just for statistics, 90 divides into 360 evenly