7.4.1. Contain at least 12 alphanumeric characters.

7.4.2. Contain both upper- and lower-case letters.

7.4.3. Contain at least one number (for example, 0-9).

7.4.4. Contain at least one special character (for example,$%^&*()_+|~-=\`{}[]:";'<>?,/).

8. Password Examples

8.1. BAD Examples

8.1.1. A password containing a single dictionary word (for example, Password).

8.1.2. Contains personal information (for Example, Birth Date, Birth Year, Family Names, Pet Names).

8.1.3. Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

8.1.4. Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

8.1.5. Contain a common word spelled backwards, preceded, or followed by a number (for example, terces, secret1 or 1secret).

8.1.6. Some variation of “Welcome123” “Password123” “Changeme123”.

9. Administrator Enforced Policies

9.1. All Network Claims Assessors systems administrators are responsible for ensuring that the network environment and all Operating Systems within Network Claims Assessors network are configured to support this password policy. The following configuration settings must be applied to all Active Directory Forests, Active Directory Domains, Windows member servers and Non-Windows servers which operate within any of Network Claims Assessors owned networks.

9.2. Enforce Password History – This must be set to 10 passwords remembered, i.e.: The user may not be able to use his/her previous 10 passwords.

9.3. Maximum Password Age – This must be set to 60 calendar days, so that the system enforces the change of the user's password every 60 calendar days.

9.4. Minimum Password Age – This must be set to 10 calendar days, so that users can only change their passwords at will every 10 calendar days.

9.5. Minimum Password Length – This must be set to 12 characters.

9.6. Password Complexity – Must be enabled to ensure that passwords are case sensitive, alpha-numeric and contain special characters.

9.7. Account Lockout Duration – Lockout duration should be set to 30 minutes.

9.8. Account Lockout Threshold – Lockout Threshold should be set to 5 bad consecutive password attempts.

9.9. Reset Account Lockout Counter – Reset Account Lockout Counter should be set to 30 minutes.

9.10. IT Administrators need to update the password blacklist annually. The blacklist needs to be recorded, approved, and communicated by the IT manager.

10. SuperUser / Administrator Passwords

10.1. A Super User / Administrator account is a highly sensitive account and extreme caution should be taken when dealing with these accounts.

10.2. Superuser or Administrator passwords should never be shared with anyone inside or outside the organization.

10.3. All Administrators will be issued with a named Administrator account. Named administrator accounts will reflect the name of the person responsible for that specific

account. The user will be responsible for their Administrator account and the safekeeping of the account password.

10.4. All Administrators will be held responsible for the activities on their set account.

10.5. All Administrator accounts must be enrolled, if supported by the system, with MFA Multi-Factor Authentication, the preference of the MFA options is, in order:

10.5.1. Authentication App

10.5.2. Phone Call

10.5.3. Alternate Email address\

10.5.4. SMS

11. Default Administrator Passwords

11.1. The default Administrator account usernames must be changed, where possible.

11.2. The default Administrator account password must be changed during the implementation of the system.

11.3. The passwords for the default administrator account should only be accessible to authorized personnel.

11.4. Passwords for Default Administrator accounts will be changed annually and must be documented within the Access control framework document and stored in a secure location, this document should not be saved on any system within Network Claims Assessors network.

11.5. Passwords for default Administrator accounts should comply with the below rules, where applicable:

11.6. Minimum Password Length – This must be set to 20 characters.

Thys Botes

MD (Network Claims Assessors)

11.7. Password Complexity – Must be enabled to ensure that passwords are case sensitive, alpha-numeric and contain special characters.

12. Local Administrator Passwords

12.1. The "Local Administrator Password Solution" (LAPS) provides the management of local account passwords of domain-joined computers. Passwords are stored in Active Directory and protected by ACL, so only eligible users can read it or request its reset.

12.2. Users who are eligible to read the local administrator passwords are responsible for the safekeeping of the passwords.

12.3. Local Administrator passwords must not be shared with any unauthorized person.

12.4. Local Administrator passwords must be changed every 90 days.

12.5. LAPS must be enrolled on all domain-joined devices.

13. Mobile Phone Passwords

13.1. Mobile phones that are used to access company information must comply with the Minimum Access Policy and must have a password set and must comply with the below:

13.1.1. Minimum Password Length must be 4 characters.

13.1.2. Password Complexity – Complex numeric, repeated, or consecutive numbers, such as "1111" or "1234", aren't allowed.\

13.1.3. Maximum minutes of inactivity before a password is required – 5 minutes.

14. Password Managers

14.1. The use of password managers has become more common, and the use of password managers is accepted within the environment, but must comply with the following:

14.1.1. Password Managers need to be enrolled with your company-issued email address.

14.1.2. Storing company passwords on a Password Managers enrolled with a personal email address is strictly prohibited.

14.1.3. Multi-factor authentication must be enabled on the account.

14.1.4. These accounts should never be shared with other internal or external parties.

14.1.5. Individual Passwords may be shared through the Password Manager application and must be controlled through the Password Manager Application.

14.1.6. Shared Passwords must be reviewed on a regular basis.

14.1.7. The use of a password generator is allowed, but the password must meet the password requirements specified in section 2.5 of this document.

15. Enforcement

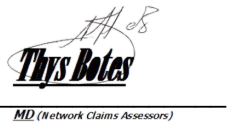
15.1. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Network Claims Assessors.

16. Definitions

TERMS	DESCRIPTION
Dictionary attacks	An attempt to gain illicit access to a computer system by using a very large set of words to generate potential passwords.

Thys Botes
MD (Network Claims Assessors)

Local Administrator Password Solution (LAPS)	For environments in which users are required to log on to computers without domain credentials, password management can become a complex issue. Such environments greatly increase the risk of a Pass-the-Hash (PtH) credential replay attack. The Local Administrator Password Solution (LAPS) provides a solution to this issue of using a common local account with an identical password on every computer in a domain. LAPS resolves this issue by setting a different, random password for the common local administrator account on every computer in the domain. Domain administrators using the solution can determine which users, such as helpdesk administrators, are authorized to read passwords.
SuperUser / Administrator	A user of a computer system with special privileges needed to administer and maintain the system

CEO name THYS BOTES CEO signature 

Signed at PAROW on this 12 day of APRIL 2022