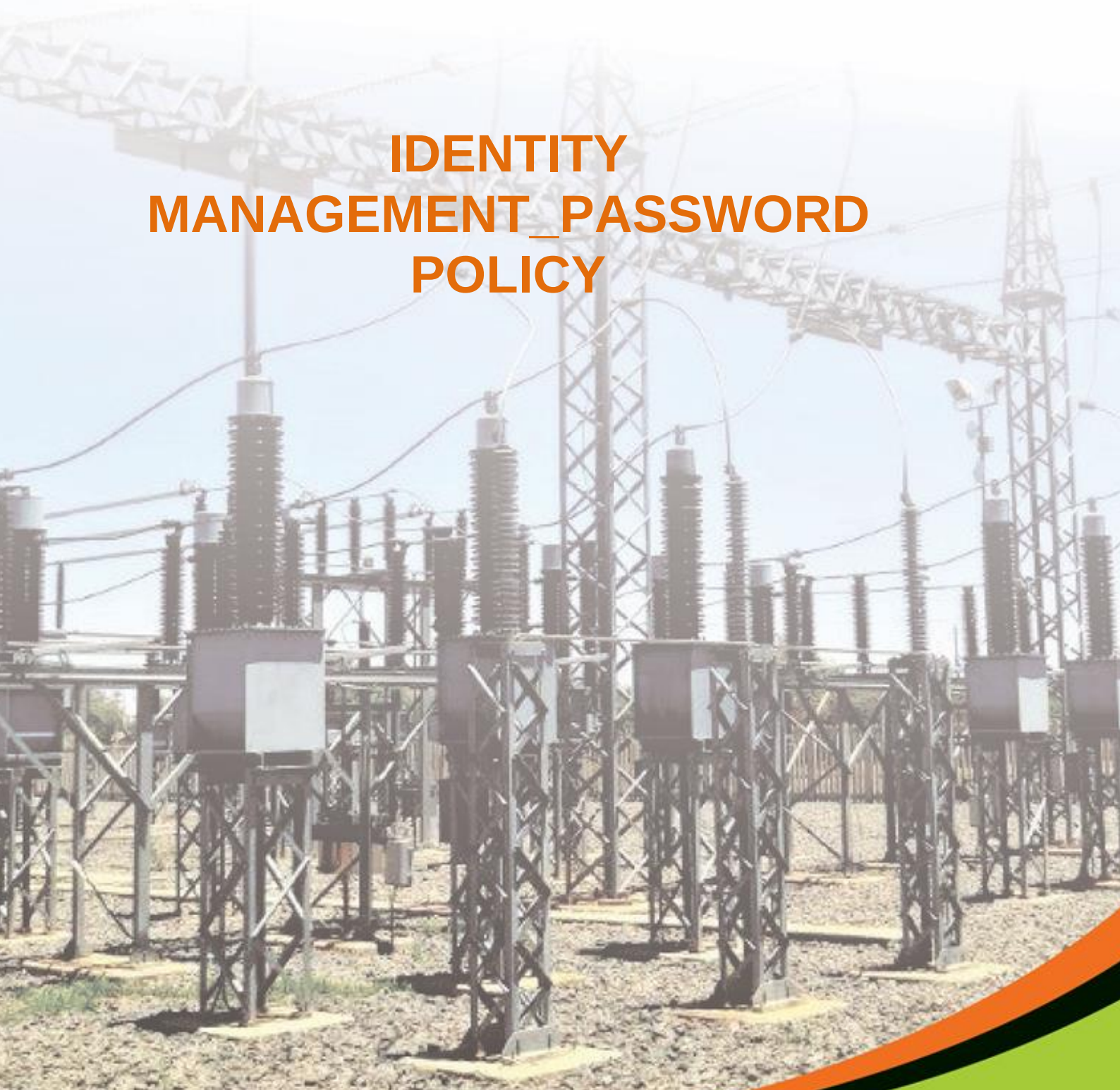
MANGAUNG
AT THE HEART OF IT ALL

CENTLEC
Reg No. 2003/011612/30

IDENTITY MANAGEMENT_PASSWORD POLICY



DIRECTORATE: OFFICE OF THE CEO	
SUBJECT: IDENTITY MANAGEMENT_PASSWORD POLICY	POLICY NO:
REV NO: 0- New	REV DATE : 31 MAY 2023
SUB-DIRECTORATE:	BOARD ITEM NO:
SIGNATURE :	
DATE APPROVED:	EFFECTIVE DATE:

1. DEFINITIONS

Password/Passphrase - refers to a sequence of characters, words or other text used to control access to a computer system, program or data.

Password history - describes a log of expired passwords, used primarily for automatic comparison with proposed new passwords.

System - describes the CENTLEC ICT Board of Directors, the system office, the government systems, besides any part or combination thereof.

User - refers to any individual, including but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using system information resources, whether or not the user is affiliated with the system.

2. OBJECTIVES

This policy is designed to protect Centlec (SOC) Ltd resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

3. POLICY PRINCIPLES

3.1 All employees and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

3.2 The following principles regarding password protection must be adhered to at all times:

3.2.1 Never write passwords down.

3.2.2 Never send a password through email.

3.2.3 Never include a password in a non-encrypted stored document.

3.2.4 Never tell anyone your password.

3.2.5 Never reveal your password over the telephone.

3.2.6 Never hint at the format of your password.

3.2.7 Never reveal or hint at your password on a form on the internet.

3.2.8 Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.

3.2.9 Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://

3.2.10 Report any suspicion of your password being broken to ICT office.

3.2.11 If anyone asks for your password, refer them to your ICT office.

3.2.12 Don't use common acronyms as part of your password.

3.2.13 Don't use common words or reverse spelling of words in part of your password.

3.2.14 Don't use names of people or places as part of your password.

3.2.15 Don't use part of your login name in your password.

3.2.16 Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.

3.2.17 Be careful about letting someone see you type your password.

3.2.18 Make use of passphrase password

4. PASSWORD REQUIREMENT

Rules for setting of password must not be too difficult as this has likelihood to decrease security if users decide the rules are impossible or too difficult to meet.
If passwords are changed too often, users may not attempt to write them down or make their password a variant of an old password which an attacker could guess.

The following minimum password requirements will be set by the ICT services:

1. Minimum and Maximum Length (number , caps , special characters and recommended characters) (8)
2. Minimum complexity – (e.g the types of characters that may be used) (number , caps , special characters and recommended characters) (8)
3. Password history – (e.g require a number of unique passwords before an old password may be reused) 30 Day remembrance
4. Maximum and Minimum password age (30) Days
5. Account lockout threshold (e.g 3 failed login attempts)
6. Account with (90) days without login should be deactivated

5. NETWORK DOMAIN PASSWORD

This section applies to Microsoft Windows network domain and shared folders, desktops, laptops, tablets, servers, and databases, including for the domain and the local password policies.

The following domain policy settings must be enforced, as a minimum:

1. Password history: 10 last passwords used
2. Maximum password age: 30 days
3. Minimum Password age: 1 day
4. Minimum password length: 8 characters for regular users
5. Minimum complexity: (number , caps , special characters and recommended characters) (8)
6. Account lockout duration:10-15 minutes
7. Account lockout threshold: 3 attempts

6. SOFTWARE APPLICATION PASSWORD

6.1 Application passwords must rely on network domain credentials where possible (Windows Integrated Security). Ref. 4 sub 2

6.2 User accounts with privileges, and systems or application accounts (accounts not attributed to a physical person):

6.2.1 At least 12 characters long and require the use of both uppercase and lowercase characters, numbers, as well as non-alphabetical characters (such as punctuation characters, Unicode, or non-printable characters)

6.2.2 Account lockout duration: 10-15 minutes

6.2.3 Account lockout threshold:-3 attempts

NOTE: Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared. Administrator account should expire every (30) days. Default Administrator account cannot be used in all the systems.

7. GUIDELINES REGARDING PASSWORD USE

Users must protect their passwords from unauthorized use and must not share passwords with others.

Users must use a password or passphrase that is longer that 8 characters inclusive with special characters.

Passwords or passphrases must be changed at least every 30 days. User will send the password reset form to ICT. Or user will have password reminder through the Active directory for self-set password after 30 days expiry. This password should comply with the password complexity set in this policy.

8. RESPOSNIBILITIES

ICT Administrator should perform password reset for the users through approved user password form.

Users can reset their password when reminded by the system.

9. ENFORECEMENT

Since password security is critical to the security of the entity and everyone, employees must ensure that the comply with the security for purpose of CENTELC data protection.

10. PROHOBITION OF PASSWORD

The following words or characters must not be used when selecting a password:

10.1 Names such as family names, username, equipment name, make or model

10.2 Repeated letters or numbers used in a sequence (1234, 0000, aaaa, 8888, etc.)

10.3 Numerical year or month abbreviations (2013, 2014, jan, feb, mar, apr, etc.)

10.4 The words “password”, “iloveyou”, “ilovegprc”, “admin”, “guest” “trustno1”, and “letmein”.

11. REVIEW AND APPROVAL

This policy and underlying strategies will be reviewed at least annually, or as necessary, to ensure its continued application and relevance.

Prepared by:

Signed:_____

Acting Executive Manager: Engineering Retail

Date:_____

Supported by:

Signed:_____

Chief Executive Officer

Date:_____

Approved by:

Signed:_____

Chairperson of the IT Governance Committee

Date:_____