P.O. Box 6082, Willemstad, Curaçao – Telephone: +1 (631) 480 2118 (USA) / +599 9 523 2685 (Curacao)

Password Construction Guidelines

Document version: 01-2023

1 – Purpose

Passwords are a critical component of information security. Passwords serve to protect access to user accounts, data and systems. However, a poorly constructed or easily guessed password can compromise the strongest defenses. This guideline provides best practices for creating strong passwords.

2 – Scope

This guideline applies to CUN students, employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords, including but not limited to user-level accounts, system-level accounts, web-accounts, e-mail-accounts, screensaver protection, voicemail and local router logins.

3 – Policy

Strong passwords are long, the more characters a password has the stronger it is. We recommend a minimum of eight characters in all work- and study-related passwords, including lower case characters, capitals, numerals and interpunction-symbols. In addition, we encourage the use of passphrases; passwords made up of multiple words. Examples include "*It's-time-for-vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type yet meet the strength requirements.

Password cracking or guessing may be performed on a periodic or random basis by CUN's ICT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4 – Policy compliance

CUN will verify compliance to this policy through various methods, including but not limited to password cracking exercises, business tool reports and internal and external audits.

Any exception to the policy must be approved by CUN's ICT Department in advance.

Any user found to have violated this policy may be subject to disciplinary action

5 – Revision History

Date of Change	Summary of Change
January 1, 2023	