P.O. Box 6082, Willemstad, Curaçao – Telephone: +1 (631) 480 2118 (USA)

Password Protection Policy

Document version: 01-2023

1 – Purpose

Passwords are a critical aspect of computer security. A weak or compromised password can result in unauthorized access to our most sensitive data and/or exploitation of our resources. All users of CUN's electronic systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for the secure use and protection of all work- and study-related passwords.

2 – Scope

The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CUN facility, has access to the CUN network or stores any non-public information on CUN's network and systems.

3 – Policy

3.1 – Password creation and use

1. All user-level and system-level passwords must conform to the Password Construction Guidelines.
2. Users must use a separate, unique password for each of their work- or study-related accounts. Users may not use any work- or study-related passwords for their own, personal accounts.
3. Users are allowed to use authorized, approved password managers to securely store and manage all their work related passwords, to the discretion of CUN's ICT Department.
4. User accounts that have system-level privileges, granted through group memberships or programs such as the Linux 'sudo' authentication-method, must have a unique password from all other accounts, held by that user, to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

3.2 – Password security and change

1. Passwords should be changed only when there is reason to believe a password has been compromised or fails to meet our Password Creation Requirements. We do not recommend the use or setting of regular password expiration.
1. Passwords must not be shared with anyone, including fellow students, friends and relatives, faculty, supervisors and colleagues. All passwords are to be treated as sensitive, confidential information. CUN recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
2. Passwords must not be inserted into e-mail messages or other forms of electronic communication, nor revealed over the phone to anyone.
3. Passwords may be stored only in password managers, authorized by CUN's ICT Department.
4. Do not use the "Remember Password" feature of applications (for example web-browsers and e-mail clients).
5. Any individual suspecting that their password may have been compromised must report the incident to CUN's ICT Department and change all relevant passwords.

3.3 – Application development

Application developers must ensure that their programs contain the following security precautions.

1. Applications must support authentication of individual users, not groups.

2. Applications must not store passwords in clear text or in any easily reversible form.
3. Applications must not transmit passwords in clear text over the network.
4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

3.4 – Multi-factor authentication

Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work- and study-related accounts, but personal accounts too.

3.5 – Policy compliance

CUN’s ICT Department will verify compliance to this policy through various methods, including but not limited to, business tool report and internal and external audits.

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

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

3.6 – Revision History

Date of Change	Summary of Change
January 1, 2023	