Password Policy

1. Context

Strong passwords are an integral component to keeping our customer's data and company data safe and protecting our infrastructure from malicious attacks. As such, every team member is to take proper care when choosing their password.

This document outlines the requirements every team member needs to follow when setting passwords for any digital account afiliated in any way with MENU. This includes, but is not limited, to all online services, as well as all electronic devices set up for use at MENU (for example PCs, network equipment).

2. Password Requirements

Each password you set needs to comply with the following minimum requirements:

- At least 8 characters in length
- Include at least one number (0-9)
- Include at least one letter (a-z)

Your password is not allowed to:

- Have a personal connection to you (e.g. your pet's name, your child's birthday)

Additionally, we recommend adding the following components to your password:

- Include at least one special character (for example .,/&%$)
- Use a passphrase: A passphrase is a sequence of words with or without connection to each other. They lead to longer passwords that are harder to crack

MENU Technologies AG · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app

Internally-developed company applications (for example the MENU platform incl. mobile, web app & back-end system) are built with those password requirements in mind, making sure that no user can set up an account without complying with aforementioned requirements.

Where possible, MENU-provided online services (for example GSuite) are also configured with the same password requirements.

Nevertheless, each team member needs to be aware that it is not possible for us to configure password requirements for every provided online service (if functionality is not available) and it is not possible for us to set software-level password requirements for any service you sign up for yourself (not provided by MENU). **Therefore it is the responsibility of every employee to make sure all passwords follow the given requirements.**

2.1. Keep your passwords safe

- **Never tell anyone your password:** Never tell anyone your password, no matter over the phone, via e-mail, instant message or in-person, no matter the hierarchical level, not even to IT if you need assistance with your account. IT administrators will reset your password in order to assist you.
- **Avoid reusing the same password:** Set a separate password for every account. Reusing the same password begs the risk that an attacker may gain access to all your accounts if he manages to compromise one of them (or the underlying service).
- **Don't write passwords down:** Never write down your passwords (no matter on paper, an Excel sheet etc.). If you are unable to remember your passwords, the only exception to this rule is using a Password Manager (see below).
- **Don't use "Remember password" features:** Some browsers (for example Google Chrome) and operating systems (for example iOS) offer the option to remember your password for a service, after you have entered it once. Do not make use of such features.

2.2. Other requirements

- **Default passwords:** Whenever setting up any device/software (new computer, network equipment etc.) with a default password it is required to change this password during setup.
- **One account for multiple team members:** Whereever possible each team members is to be issued a separate account with unique credentials.
  In rare cases this may not be possible (technical/system limitations). If you encounter such a case, you need to receive approval from the Security Management to use a Password Manager to share the same credentials with other team members.

3. Password Managers

Password Managers are software tools that can be installed to a device and be used as a "vault" for all your passwords.

MENU approves the following Password Managers for use:

- 1Password (https://1password.com/)

- LastPass (https://www.lastpass.com/)

The password for the Password Manager needs to follow the same requirements, as well as the password protecting the devices where you have the Password Manager installed. This means if you decide to install the Password Manager on your smartphone, your smartphone passcode needs to follow the requirements set forth above.

If you are using the same Password Manager for personal use, a separate vault/section is to be created within the Manager, in order to separate personal account passwords and company account passwords.