**INTEROFFICE MEMORANDUM**

To: Management

From: Team

Subject: Secure Passwords Guidelines

Date:

– INTENDED FOR PUBLIC DISTRIBUTION –

SECURE PASSWORDS: AN ESSENTIAL SECURITY PRACTICE

It is crucial to use secure, complex passwords. Complex passwords prevent a malicious hacker from guessing your password and gaining unauthorized access to the organization’s computers. Hackers can access your personal data or the company’s resources if non-complex passwords are used. Here are some guidelines for how to create a complex secure password

Passwords should have the following characteristics to be considered complex and secure. These characteristics come from the National Institute of Standards and Technology (NIST) security standards (<https://pages.nist.gov/800-63-3/sp800-63b.html>) and the Microsoft Security Standards (<https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>)

1. User-generated passwords should be **at least 8 characters long**, and the key space for users should support up to at least 64 characters.
2. Passwords should contain a **combination of uppercase letters, lowercase letters, numbers, and symbols**.
3. Users should be able to create passwords at least 64 characters in length.
4. Knowledge-based passwords or security questions, such as “What was the name of your first pet?” should not be used.
5. Passwords should not have hints.
6. Context-specific words, such as the name of the service for which the password will be used or the user’s specific username, should not be permitted.

To generate a secure password, users can use a passphrase-based approach. A passphrase is a more secure form of a password. People use passphrases for the same reasons and in the same way as a password. A passphrase is typically longer and contains spaces. A passphrase can also contain symbols and does not need to be grammatically correct. (As defined by Okta, a security firm: <https://www.okta.com/identity-101/password-vs-passphrase/>)

Several online sites can help you generate secure passwords and passphrases. The website <https://www.useapassphrase.com/> details how to create a secure passphrase and helps generate secure passphrases. The website [https://www.avast.com/en-us/random-password-generator](https://www.avast.com/en-us/random-password-generator#pc) details how to create a secure password, although these passwords are very complex and are hard to remember for a user.

Please contact the internal cybersecurity team with any questions on creating a secure password!

Thank you.