# Secure Password Guideline

National Centre for Information Technology

# TABLE OF CONTENT

# 1 Purpose

Passwords are the most common means for proving your identity and logging into your computer and websites or accessing information. Unfortunately, far too often people do little to protect their passwords, using simple combinations such as 12345, password, qwerty, or abc123. In other cases, people simply use their loved one’s name or their date of birth – information that can be easily found on the internet, such as on Facebook. With access to your password, an attacker can steal your digital identity, access your bank accounts, or even access your organization’s confidential information, causing a tremendous amount of harm. It is also important to remember that if someone steals your password, you could be liable for anything they do! Choosing the right password is something that many people find difficult, there are so many things that require passwords these days that remembering them all can be a real problem. This document seeks to provide the guidance for setting secure passwords.

# 2 Scope

This document has been created for the general public and any ICT user within the Maldivian Community

# 3 Setting a secure password

## 3.1 Basics

- Use at least eight (8) characters. For confidential information the recommendation is fifteen (15) characters.
- Use a random mixture of characters, upper case letters (A-Z), lower case letters (a-z), numbers (0-9), punctuation (;”_...), spaces and symbols ($@&*+...).
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.

## 3.2 Things to avoid

- Don't just add a single digit or symbol before or after a word. e.g. "apple1"

- Don’t write down the passwords.
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Don't just garble letters, e.g. converting e to 3, L or i to 1, o to 0. as in "appl3"

## 3.3 Tips for remembering passwords

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password which is related to your life or your favourite phrase, song or movie. e.g. “M@rriedW1th2Kids”, “G0neW1ththeW#nd”
- Using the first letter of each word in a sentence is much easier to remember. For example the sentence below maybe very simple to remember:

  **My 2nd son was born at Indira Gandhi Memorial Hospital at 5:30am**

  However, we can use that sentence to create the password you see here:

  **M2swb@IGMH@5:30am**

  This is a long complex password that will be very difficult to guess but easy to remember.

- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.
- Choose a password which you can remember easily for specific websites, such a password can be “http://www.f4c3b00k.c0m” for Facebook or for Skype you could use the password “http://www.5kyp3.c0m”

  ***Note:*** *Please do not set the above examples as your password. This is just an example for remembering passwords for specific websites.*

## 3.4 Bad passwords

- Don't use passwords based on personal information such as: name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number,

car registration number, address etc. This includes using just part of your name, or part of your birthdate.
- Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein", "welcome".
- Never use a password based on your username, account name, computer name or email address.
- Never set a password which is in a dictionary.

## 3.5 Changing your Password

- Change your password regularly, once a month or three months is reasonable for most purposes.
- Change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- Remember, don't re-use a password.

## 3.6 Protecting your password

Keep in mind that just having strong passwords is not enough. It does not matter if you have the most complex passwords in the world; failing to take the following steps can result in your passwords being compromised:

- Ensure that your computer is actively protected. This means making sure automatic updating is enabled and you have the latest anti-virus.
- Be sure to use different passwords for different accounts. For example, never use the same passwords for your work or bank accounts as your personal accounts, such as Facebook, YouTube, or Twitter. This way if one of your passwords is hacked, the other accounts are still safe.
- Never share your password with anyone else, including a supervisor, or an IT support professional. Remember, your password is a secret. If anyone else knows your password, it is no longer secure.
- Never use a public computer, such as at hotels or libraries, to log into an account. Since anyone can use these computers, they may be infected with a malicious code that is capturing all your keystrokes. Only log into your work or personal accounts on trusted computers you control.

- Never store your password on your computer or write it down on a paper. If you write them down, be sure to store them in locked location that only you have access to; never store them in public view.
- Never run any executable files sent by anyone on the Internet, this can be a stealer which would send the user and password stored in the browser to an attacker.
- Never tick “remember me” option in a browser while logging into a website from a different computer than your own. The password is stored in the browser and it could be retrieved.
- Never send your password via email or other unsecured channel
- Be very careful when entering your password with someone else in the same room.
- If you believe your password has been compromised or have reason to believe it is no longer a secret, contact your help desk and change your passwords immediately from a computer you control and trust.

# 4 Document Information

## 4.1 Revision History

| VERSION | EFFECTIVE DATE | DETAILS |
|---|---|---|
| 1.0 | 11.09.2012 | Initial Release |

# 5 Issuing Authority

This document has been compiled by and issued with the authority of the National Centre for Information Technology

# 6 Contact Information

Any suggestions, queries or requests for clarification regarding this standard may be forwarded to NCIT at secretariat@ncit.gov.mv