Password Policy

1. Purpose

The purpose of this policy is to establish a standard for creation, distribution, safeguarding, and reclamation of passwords, the protection of those passwords, and the frequency of change and also to establish the procedure for securely managing the passwords by University of Technology and Applied Sciences - Ibra.

2. Scope

This policy is applicable to all University of Technology and Applied Sciences - Ibra computing resources such as Desktops, Laptops, Servers, Communication equipment where University of Technology and Applied Sciences - Ibra staff manages and gains access to control.

3. Policy

General

All passwords must be constructed and implemented according to the following rules:

3.1. Passwords must be a minimum of 8 characters in length and contain characters from the following three categories:

3.1.1. Combination of upper and lower case characters (a through z and A through Z)

3.1.2. Base 10 digits (0 through 9)

3.1.3. Non-alphabetic characters (for example, !, $, #, %)

3.1.4. Example Password : Abdull@h#987

3.2. Passwords must be changed once in 90 days

3.3. Passwords must not be divulged to anyone without approval.

3.4. If the security of a password is in doubt, the password must be changed immediately.

3.5. Users are advised not to circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software.

3.6. Computing devices must not be left unattended without enabling a password protected screensaver, logging off or locking of the device within 5 minutes of idle time.

3.7. Last 5 passwords should not be reused for any reason.

3.8. After 3 unsuccessful login attempts, account shall be locked.

3.9. Password should strictly be kept private and confidential. Passwords should not be shared, coded into programs, stored in an unprotected form in any information systems or written down.

3.10. Password should not be displayed in plain text while logging in. Passwords must be masked.

3.11. Passwords should be changed immediately during suspected compromise or wrongful disclosure scenario.

Additional settings

System Passwords (PCs)

- Maintain a power-on / BIOS password for Windows /7/8/10 and grub password for Linux
- The system / user login passwords should be changed at a minimum of once in every 90 days.

File Passwords

- It is recommended that these be maintained while transferring files classified to be "Restricted" information.

Application Passwords

- Based on the application design the passwords must be set.

Hardware, Database and Network Component passwords

- Based on the available configuration of the components the passwords must be set. Change frequency is once in 6 months.
- The administrator passwords are known to few persons and securely stored and therefore the change frequency will be at least once in 6 months.

Guideline for creating a strong password

The following are recommended:

- It must adhere to a minimum length of 8 characters and above.
- It must be a combination of alpha, numeric and special characters.
- It must not be anything that can easily get tied back to the account owner such as: user name, nickname, relative's names, birth date, mobile number, etc.
- It must not be dictionary words or acronyms.
- Combine short, unrelated words with numbers or special characters. For example: eAt%42pe!N
- Do not re-use previously used passwords
- Do not use the same password for multiple accounts
- Make the password difficult to guess but easy to remember.
- Substitute numbers or special characters for letters. (But do not just substitute)

For example: livefish - is a bad password

L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and it's substituted by 1's can be guessed:

l!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable

Another Eg: liv2#f1sh

Enforcement

University of Technology and Applied Sciences - Ibra reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Any user found to have violated this policy may be subject to disciplinary action.