PASSWORD POLICY

2020-2021

HABITAT SCHOOL
AL JURF, AJMAN

Creation date: 20/5/2014
Last amendment date: 21/4/2020
Next review date: April 2023

Members of the committee

- Mr. Wasim Yousuf Bhat (Dean)
- Mr. Bala Reddy Ambati (Principal)
- Mr. Suresh Sukumar (Vice Principal)
- Mr. Hamza Kollath (Administrative Officer)
- Ms. Thasni Shahal (Software Analyst)
- Mr. Boney R (School System Administrator)
- Mr. Tanzeem Shabir (Supervisor KG)
- Mr. Sajir Kanjirampara (Supervisor Grade 9-12-Boys)
-

Introduction

Effective password management will protect Habitat School's data and reduce the risk of unauthorized applications access. The policy is to establish a secure information technology environment by enforcing the use of strong passwords. Strong and complex password are the front line of protection for user's accounts. A poorly chosen password may result in the compromise of Habitat's entire network. The purpose of this policy is to provide standards for defining domain passwords to access Habitat IT resources such as email, academic and administrative applications, computing labs and School-owned computer systems for protecting Habitat data and reducing the risk of unauthorized access by enforcing the use of strong passwords.

Scope

This policy shall apply to all employees, students, and parents of Habitat School, and shall govern acceptable password use on all systems that connect to Habitat School network or access or store Habitat School's data.

Policy

Password Creation

1. All user and admin passwords must be at least [8] characters in length. Longer passwords and passphrases are strongly encouraged.
2. Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
3. Passwords must be completely unique, and not used for any other system, application, or personal account.
4. Default installation passwords must be changed immediately after installation is complete.
5. Passwords must not include names or any other personal information about the user that might be known by others
6. Password must contain requirements such as uppercase/lowercase letters, number and special characters.

Password Aging

User passwords and system-level passwords must be changed every [6] months. Previously used passwords may not be reused.

Password Protection

1. Passwords must not be shared with anyone (including coworkers and supervisors), and must not be revealed or sent electronically.
2. Passwords shall not be written down or physically stored anywhere in the office.
3. When configuring password “hints,” do not hint at the format of your password (e.g., “zip + middle name”)
4. User IDs and passwords must not be stored in an unencrypted format.
5. User IDs and passwords must not be scripted to enable automatic login.
6. “Remember Password” feature on websites and applications should not be used.

7. All mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

8· We can use a ‘password vault’, these can store passwords in an encrypted manner and can generate very difficult to crack passwords.

9 · The account should be “locked out” following six successive incorrect log-on attempts

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

This policy is linked with all the other policies of the School.