



PASSWORD POLICY

(2023-24)

MEMBERS OF THE COMMITTEE

Ms. Mariyam Nizar Ahamed	Principal
Ms. Huma Ather	Vice Principal
Ms. Reshama Abootty	Software Analyst
Mr. Kashif	System Administrator
Ms. Nimisha Chinnakuttan	Computer Science Department

SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW

Password policy was approved by the Governing body of the school on	01/04/2020
The Implementation of this policy will be monitored by the	Password Policy committee members
Review of the policy (Monitoring will take place at regular intervals)	Annually
Last Review Date	10/04/2023
Next anticipated Review date	April 2024

PASSWORD POLICY

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

- These statements apply to all stakeholders (Staff, Students, Parents, Vendors) of Habitat School.
- All school networks and systems will be protected by secure passwords.
- All users are clearly defined with access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Administrator and will be reviewed, at least annually, by the online safety group.
- All stakeholders have a responsibility for securely keeping the login credentials. Ensure that other users are not accessing the systems using other user's login credentials. Any breach of security or suspicious incidents must be immediately reported with evidence.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the IT Administrator who will keep an up-to-date record of users and their usernames

Habitat School, Al Tallah Networks

- Habitat- For Staff
- Habitat Guest- For guest and visitors
- Habitat Corp- Corporate Staff

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.

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 co-workers 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.

Training/awareness

It's imperative to educate users about the significance of maintaining secure passwords and the potential dangers associated with unauthorized access and data loss. This applies even to the youngest users, emphasizing the importance of responsible password management. By ensuring that all stakeholders understand how passwords can be compromised, we empower them to make informed decisions and adopt secure practices to safeguard sensitive information effectively.

Members of staff will be made aware of the school's password policy

- During induction
- Through the school's online safety policy and password security policy
- Acceptable use agreement

Students will be made aware of the school's password policy

- In lessons
- Through the Acceptable Use Agreement
- Through activities

Audit/monitoring/reporting/review

The IT Administrator will maintain comprehensive records encompassing

- User Ids and requests for password changes
- User logins
- Any security incidents pertinent to this policy

Unacceptable Use

- Any breach of password policy will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate as per the reporting mechanism.

- Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take necessary action.

Enforcement

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

First violation:-

For Teaching Staff

Verbal warning by Section Head

Name of Section Head (Boys): Ms. Anjana Pillai

Email ID: sectionheadboys@tallah.habitatschool.org

Name of Section Head (Middle): Ms. Anni . M. Jones

Email ID: sectionheadmid@tallah.habitatschool.org

Name of Section Head (Primary): Ms. Neethu Jomon

Email ID: sectionheadpri@tallah.habitatschool.org

Name of Section Head (KG): Ms Swapna

Email ID: sectionheadkg@tallah.habitatschool.org

For non-teaching staff

Verbal warning by HSE

Name of the HSE officer: Christopher D'Cruze

Email ID: christopherj@tallah.habitatschool.org

Second violation:-

Memo will be issued by the Principal

Name of Principal: Ms. Mariyam Nizar Ahmed

Email ID: principal@tallah.habitatschool.org

Third violation:-

Use of any of school resources for any illegal activity will usually be grounds for summary dismissal, and the school will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

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