PASSWORD PROTCTION POLICY

Overview

Password protection is a security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information. The policy is applicable to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that belongs to WPS(Wi-Fi Protected Setup), resides at any WPS location, has access to the WPS network, or stores any WPS information.

The Governors, staff, students and parents of The Bloomington Academy, Ajman play a vital role in setting an example for the whole school and are central to implementing policy and process. It is imperative that a whole school community approach to password policy is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe learning. This supports a robust online safety ethos and ensures that the school is providing the best online safety provision they possibly can.

Scope of Password Security Policy

The school will be responsible for ensuring that the school network is safe and secure as possible and that procedures within this policy are implemented. A safe and secure password system is applied to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).To ensure the online safety of the stakeholders, a strong password system is mentioned.

Policy Procedures

The Bloomington Academy, Ajman Password Policy includes: -

I) Password Creation / Sharing Policy:-

1. All the password will be created and issued by the IT Admin as per the request of staff members.
2. The school official parent communication platform which has been activated when the child enrolled in campus and the IT Admin is responsible for future communications
3. The VLE passwords are created by the ICT teacher as per the instructions getting by the IT Admin.
4. While constructing the password for VLE, an option strictly maintained to change the first sign in.
5. All our school network connected devices such as Laptops, LED Panels, Printers etc. were set up with the strong password.
6. All the Users are trained about password protection and the password policy that implemented.
7. IT systems are configured to prevent password reuse.
8. Passwords on their expiry shall cease to function

9. All user accounts are protected by strong passwords and that the strength of the passwords meets the security requirements of the system as follows.
10. We are ensuring the safe and secure password sharing system to circulate all the stakeholders which has been created by the IT Admin/ in charges.
11. While sharing the password, we are instructing the stakeholders to reset their password when they first sign in.
12. The VLE passwords are shared to the stakeholders through the any of our official communication system.

Instruction for creating the password

1. Should contain 8 characters
2. Should contain alpha numeric characters
3. Should include special character (e.g., ~, !, @, #, $, ^, (,), _, +, =,-,?,)
4. Contain at least one number (e.g., 0-9)
5. Should contain upper- & lower-case characters (Aa – Zz)
6. Should not include personal data
7. Should not repeat any characters more than twice
8. Should not contain a dictionary word in any language, slang, dialect, jargon, etc

II) Reset Password / Deleting Password :-

1. IT Admin is the overall in charge to manage and implement all the password related issues.

2. We implemented the account lockout strategy in VLE. This shall be based on a risk analysis of the system to trying with more than two wrong attempts the system will automatically locked and the user must contact the IT Admit resetting the password

3. All passwords will meet the following criteria:
4. All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
5. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days. - Passwords must NOT be inserted into email messages or other forms of electronic communication.
6. All user-level and system-level passwords must conform to the guidelines described below
7. If any of the stakeholders are resigning from our organization, we will make sure that to delete all the accounts related to the concern person will be removed from our domain and ensure our data security.

III) Password Maintenance Policy: -

1. Don't reveal your password over the phone to ANYONE
2. Don't reveal your password to any supervisor
3. Don't reveal your password in an email message
4. Don't talk about your password in front of others
5. Don't hint at the format of your password (e.g., "my family name")
6. Don't reveal your password on questionnaires or security forms
7. Don't share your password with family members
8. Don't reveal your password to your friends
9. Don't write passwords down and store them anywhere.
10. Don't store passwords in a file on ANY computer system
11. Don't use the "Remember Password" feature or the "Remember Me" on any application that contains sensitive data.
12. Don’t use the same password for more than one account.

Policies Implementation: April 2020

Review Date: August 2023

Next Review Date: As Required