TechnoHacks EduTech Password Policy

Objective: The primary goal of TechnoHacks EduTech password policy is to ensure the security of our digital assets and protect sensitive information. This policy aims to enforce strong and unique passwords to mitigate the risk of unauthorized access and potential security breaches.

Password Composition:

Length:Minimum of 12 characters.
Maximum of 20 characters.

Character Requirements:

Include at least one uppercase letter.
Include at least one lowercase letter.
Include at least one numerical digit.
Include at least one special character (e.g., !, @, #, $).

Password Expiry:

Passwords must be changed every 90 days. Users will be prompted to change their passwords on their next login if the password is about to expire.

Password History:

Users cannot reuse their last 5 passwords.

Account Lockout:

After 3 consecutive failed login attempts, the account will be locked for a period of 15 minutes.
Users can contact the IT helpdesk to unlock their accounts if needed.

Two-Factor Authentication (2FA):

Enforce 2FA for all accounts, especially for privileged and sensitive roles.
2FA methods may include SMS, authenticator apps, or hardware tokens.

Account Access:

Employees should **not** share their passwords with anyone, including IT support or supervisors.
Never write down passwords or store them in easily accessible locations.

User Education:

Regularly conduct security awareness training for employees to educate them about the importance of strong passwords and security best practices.

Password Creation Tips for Users:

Avoid easily guessable information such as birthdays, names, or common words.
Do not use the same password across multiple platforms or services.
Consider using passphrases that are easy for you to remember but difficult for others to guess.
Regularly update passwords even if not prompted for a change.

Policy Enforcement:

Periodic audits will be conducted to ensure compliance with the password policy.
Non-compliance may result in temporary account suspension, mandatory password reset, or other appropriate disciplinary actions.
Review and Updates: This password policy will be reviewed annually and updated as necessary to align with evolving security threats and best practices. Employees will be notified of any changes to the policy in a timely manner.