PASSWORD POLICY

CONTENTS

LIST OF ABBREVIATIONS (OR) SYMBOLS

BYOD	Bring your own device
PIN	Personal identification number

DEFINITION OF PASSWORD

Password protection is a security process that protects information accessible via computers that need to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.

BY THIS POLICY

This policy is for guiding create better and stronger passwords to protect your information, computer access, sensitive {company} documents and files, preventing to breaches, compromising {company} anything that could harm you or {company} in anyway.

APPLIES TO

All employees, students and other workers at {company}. Including all Websites and account to own personal accounts, also {company} accounts login outside of {company} environments. This guideline applies to all passwords including user, system and web privileges access, email accounts and et.

POLICY GUIDELINES

Password Creation

The best methods for secure passwords:

- The user and system accounts passwords must follow the password creation guidelines, do not use the same password for {company} and for non-{company} accounts. Accounts that have system privileges granted through group memberships or programs such as ROOT must have a more secure unique password and 2-step verification.

- Preferable password should contain upper- and lower-case letters, multiple numbers from 0-9 and distinctive character such as, “! $%^&*() _+|~-=\`{}[]:";'<>?,/ ”.
- You can also use the long sentences from your favourite book like 32 characters with spaces in it at Harry Potter example which is easier to remember.

Poor, or weak, passwords have the following characteristics:

- Contain less than 15 characters, can be found in an any kind dictionary, including foreign language, or exist in language slang, dialect, or jargon.
- Contain personal information such as Birthdate, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters, work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as “aaabbb”, “qwerty”, “zyxwvuts”, or “123321”, frequently used words spelled backward or preceded or followed by a number (for example, “terces”, “secret1” or “1secret”).

Password Change

- The user and system accounts passwords including email, web, desktop computer, root, enable, NT admin, application administration accounts et cetera. The recommended change is after published news about data breaches and information leaks even you are not affected by this just to be sure that your account remaining secure, on corporate these are set to be change 90-180days at {company} and school is 90 days.
- Password cracking or guessing may be performed on a periodic or random basis by the Information Security team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be following the password creation guidelines.

Password Protection

- {company} and personal passwords should not be shared with anyone including administrative assistants, managers, co-workers, and family members. Passwords are confidential information and should keep private.
- Passwords should not be inserted into email messages, not be revealed over the phone to anyone and on questionnaires or security forms.
- Do not hint at the suggestions of a password what would it be as family names and year of graduation, do not use the remember password feature for applications and any logins.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices without encryption and for browser local storage.
- User suspecting that password may have been compromised must report the incident and change all passwords. Students and employees' access to company data is limited based on user profiles defined by System administrators and automatically enforced.

Application Development Security

Application developers must ensure that their programs contain the following security implements:

- Supporting 2-step authentication to individual user verification code.
- Not storing passwords in clear text or in any easily reversible form, transmitting passwords in clear text over the network and it should not be displayed on the screen when they are being entered.
- Ask users to change their password at their first logon.
- Automatically 'lock' a user account after a defined number of consecutive failed login attempts.
- Students and employees' access to company data is limited based on user profiles defined by System administrators and automatically enforced.

POLICY COMPLIANCE

Exceptions

Any exception to the policy shall be approved by the information security manager in advance.

Non-Compliance

Students and employees found to have violated this policy may be subject to disciplinary action.

REVISION HISTORY

Version	Description	Date	Author	Approved By
1.0	Initial version	14/04/2025	ztothez	