

IT Password Policy

POLICY STATEMENT:

Purpose

The purpose of this policy is to ensure the security of our systems and protect sensitive information from unauthorized access. This policy outlines the requirements for creating strong, secure passwords.

1. Password Length and Complexity

All passwords must meet the following minimum requirements:

- **Minimum Length:** Passwords must be at least **8 characters** long.
 - **Password Complexity:** Simple passwords such as "password123" or "admin123" are strictly prohibited.
-

2. Recommended Password Creation Method

To improve password security, it is **strongly recommended** that staff create passwords by combining **three random words** from the dictionary. This method ensures that the password is both complex and easier to remember.

Alternatively, staff may use a **trusted password manager or an online password generator** to create secure passwords.

3. Prohibited Passwords

The following types of passwords are prohibited:

- Common or easily guessable passwords (e.g., "password," "123456," "admin").
 - Personal information such as names, birthdays, or company-related terms.
 - Sequences or repeated characters (e.g., "abcdefg," "qwerty").
-

4. Password Uniqueness

Each password must be **unique** and should not be reused across multiple accounts or systems. Reusing passwords increases the risk of security breaches.

5. Password Changes

While regular password changes are not mandatory, passwords should be updated if there is any suspicion of compromise, or when instructed by IT/security teams.

Policy Owner: Managing Director

Stage of Approval: Approved

Date of Review: April 2025

6. Responsibility

It is the responsibility of each staff member to ensure their passwords are kept secure. Passwords should never be shared, written down in accessible locations, or stored insecurely.

Compliance

Failure to comply with this policy may result in disciplinary action as per the organization's IT security protocols.