# Password Policy and Employee Responsibilities

## Password Policy

Employees are required to create passwords that are sufficiently strong to protect company data. Passwords should be unique, contain a mix of letters, numbers, and symbols, and be changed on a regular basis. Reusing old passwords or using obvious words such as 'password' is discouraged. The company may enforce minimum length and complexity requirements to ensure consistency and reduce risks.

## Employee Responsibilities for Data Protection

All employees share responsibility for safeguarding company information. This includes ensuring that devices are locked when unattended, avoiding the sharing of passwords, and reporting any suspicious activity to the IT team promptly. Employees are also expected to handle sensitive data carefully, both in digital and physical form, and comply with company policies regarding data usage, storage, and sharing.