# Basic Security Policy for Small Office Setup

## 1. Password Policy

* All employees must use **strong passwords** containing at least **12 characters**, including uppercase and lowercase letters, numbers, and special characters.
* Passwords must be **changed every 90 days**.
* Multi-factor authentication (MFA) must be enabled where applicable.
* Employees must not **share passwords** or write them down in unsecured locations.

## 2. Data Backup Policy

* Critical business data must be **backed up daily** and stored in a secure location.
* Backups should be maintained in both **cloud storage** and **external hard drives**.
* Backup copies must be **encrypted** and **password-protected**.
* Only authorized personnel should have access to backup storage systems.

## 3. Internet Usage Guidelines

* Office internet should be used **only for business-related activities**.
* Employees must not access or download **unauthorized software** or visit **malicious websites**.
* Social media usage should be limited to **work-related purposes**.
* All devices must have **up-to-date antivirus and firewall protection**.
* Employees should avoid clicking on **suspicious emails or links** to prevent phishing attacks.
* Use of public Wi-Fi for accessing office systems is strictly prohibited unless a **VPN** is used.