Periwinkle Public Relations Ltd Information Security Policy

(Password & Access Controls, Mobile Device Encryption, and Security Systems)

1. Purpose

This policy sets out the organisation's requirements for secure access, password management, mobile-device protection, and the technical and organisational measures used to safeguard information. It supports compliance with UK legislation including the **UK GDPR**, **Data Protection Act 2018**, and recognised good practice such as **NCSC Cyber Essentials** and **ISO 27001 principles**.

2. Scope

This policy applies to:

- All employees, contractors, and third parties with access to company systems
- All company-owned or BYOD devices used for business purposes
- All information assets, whether stored electronically or physically

3. Roles and Responsibilities

- **Senior Management**: Ensures appropriate resources and oversight.
- **IT / Security Lead**: Implements controls, monitors compliance, and manages access.
- **All Users**: Must follow this policy and report security concerns immediately.

4. Password & Access Management Requirements

4.1 Password Standards

All passwords used to access company systems must meet the following minimum requirements:

- Minimum length: **12 characters**
- Must include a mix of letters, numbers, and symbols
- Must not include personal information (names, birthdays, etc.)
- Must be unique and not reused across systems
- Must not be shared with any other individual

Where supported, **passphrases** (e.g., "CorrectHorseBatteryStaple") are recommended.

4.2 Multi-Factor Authentication (MFA)

MFA is **mandatory** for:

- Email and cloud services
- Remote access (VPN, remote desktop, etc.)
- Administrative accounts

- Any system containing personal or sensitive data

4.3 Account Management

- Access is granted on a **least-privilege** basis.
- New accounts require formal approval.
- Accounts are reviewed **quarterly** for appropriateness.
- Accounts for leavers are disabled **within 24 hours** of termination.
- Shared accounts are prohibited except where technically unavoidable and approved.

5. Mobile Device & Encryption Requirements

5.1 Device Security

All mobile devices (laptops, tablets, smartphones) used for company business must have:

- **Full-disk encryption** enabled (e.g., BitLocker, FileVault, Android/iOS native encryption)
- **Automatic screen lock** after 5 minutes of inactivity
- **Strong device passcodes** (minimum 6-digit PIN or equivalent)
- **Remote wipe capability** for lost or stolen devices
- **Up-to-date operating systems and security patches**

5.2 Bring Your Own Device (BYOD)

Where BYOD is permitted:

- Devices must meet the same encryption and security requirements as company devices
- Company data must be stored in **managed, segregated containers** (e.g., MDM workspace)
- Users must agree to remote wipe of company data if the device is lost or compromised

6. Appropriate Security Systems

6.1 Technical Controls

The organisation maintains appropriate security systems including:

- **Firewalls** protecting all networks
- **Anti-malware and endpoint protection** on all devices
- **Email filtering** to block phishing and malicious attachments
- **Secure configuration** of all servers, laptops, and cloud services
- **Regular patching** of operating systems and applications
- **Encrypted backups** stored securely and tested regularly

6.2 Monitoring & Logging

- System access and administrative actions are logged.
- Logs are retained for a minimum of **12 months**.
- Alerts are generated for suspicious activity, repeated login failures, or unauthorised access attempts.

6.3 Data Transmission Security

- All data transmitted externally must use **TLS/HTTPS** or equivalent encryption.
- Sensitive data must not be sent unencrypted via email.
- Portable media (USBs, external drives) must be encrypted or avoided.

7. Incident Reporting & Response

All users must report:

- Lost or stolen devices
- Suspected phishing attempts
- Unauthorised access
- Malware infections

Reports must be made **immediately** to the IT/Security Lead. Incidents will be investigated and documented in line with the organisation's Incident Response Procedure.

8. Policy Compliance

Failure to comply with this policy may result in disciplinary action and removal of system access. This policy is reviewed **annually** or following significant changes to systems, legislation, or risk.