IT POLICY CHECKLIST

1. Staff Computer Use Policy □

Define acceptable use of company computers and technology.

2. Information Security Policy □

Outline procedures to protect sensitive data from unauthorised access, breaches, and other security threats.

3. Privacy Policy □

Establish guidelines for collecting, storing, and processing personal information in compliance with data protection regulations.

4. Local Admin Policy □

Restrict administrative privileges on devices to prevent unauthorised changes and reduce the risk of malware or system misconfigurations.

5. Password Policy □

Enforce strong password creation, management, and periodic changes to protect accounts and systems from unauthorised access.

6. Removable Media Policy □

Govern the use of USB drives, external hard drives, and other removable media to minimise risks of data loss or malware infections.

7. Security and Privacy User Responsibilities □

Educate employees on their role in maintaining security and privacy, including safe internet habits and reporting suspicious activities.

8. Service Account Audit Process □

Ensure service accounts used by applications or systems are regularly reviewed, properly managed, and not misused.

9. User Account Review Process □

Periodically review user accounts to confirm access rights align with current job responsibilities and remove inactive accounts.

10. Security Incident Response Plan □

Detail the steps to detect, respond to, and recover from security incidents, ensuring minimal impact on business operations.

11. Anti-Malware Policy □

Establish measures to detect, prevent, and mitigate malware threats through regular updates and scanning protocols.

12. Data Protection Policy □

Describe how data is securely stored, accessed, and shared, protecting it from loss, corruption, or unauthorised access.