Cybersecurity Checklist for Small Businesses

1. Network Security

[ ] Firewall: A firewall is installed and configured to filter traffic.

[ ] Router Security: Default passwords and settings on routers are changed.

[ ] Secure Wi-Fi: Wi-Fi networks are encrypted with WPA3 or WPA2.

[ ] Virtual Private Network (VPN): VPN is used for remote access and secure communication.

[ ] Network Segmentation: Critical systems and sensitive data are on separate networks.

2. Endpoint Security

[ ] Anti-Malware/Anti-Virus: All devices have updated anti-malware/anti-virus software.

[ ] Operating System Updates: Operating systems on all devices are up to date.

[ ] Software Patching: All applications and software are regularly updated.

[ ] Device Encryption: Sensitive data on devices (like laptops) is encrypted.

[ ] Mobile Device Management (MDM): Policies are in place for securing mobile devices.

3. Access Control

[ ] Password Policy: Strong password policies are enforced (e.g., length, complexity).

[ ] Multi-Factor Authentication (MFA): MFA is used for critical systems and services.

[ ] Role-Based Access Control (RBAC): Access to data and systems is granted based on roles.

[ ] Least Privilege: Users have the minimum access necessary for their roles.

[ ] User Account Management: Inactive accounts are disabled or deleted promptly.

4. Data Protection

[ ] Data Backup: Regular backups are taken and stored securely (off-site or in the cloud).

[ ] Sensitive Data Handling: Sensitive data is encrypted/protected during storage and transmission.

[ ] Data Retention Policy: There is a clear policy for retaining and disposing of data.

[ ] Data Loss Prevention (DLP): Tools or policies are in place to prevent data leaks.

[ ] Third-Party Data Sharing: Agreements and assessments ensure third-party security.

5. Physical Security

[ ] Physical Access Control: Access to server rooms or sensitive areas is restricted.

[ ] Security Cameras: Cameras monitor critical areas, with appropriate data protection.

[ ] Secure Disposal: Hardware and sensitive documents are securely disposed of.

6. Employee Training & Awareness

[ ] Security Awareness Training: Regular training on cybersecurity best practices.

[ ] Phishing Simulations: Phishing exercises to test employee awareness.

[ ] Incident Reporting: Clear channels for reporting suspicious activity.

[ ] Social Engineering Awareness: Training on identifying and avoiding social engineering attacks.

7. Incident Response and Business Continuity

[ ] Incident Response Plan: A documented plan for responding to security incidents.

[ ] Designated Response Team: A team or individuals responsible for managing incidents.

[ ] Business Continuity Plan: A plan for maintaining business operations during disruptions.

[ ] Disaster Recovery Plan: A plan for restoring critical systems after a disaster.

[ ] Regular Drills and Testing: Incident response and business continuity plans are tested regularly.

8. Compliance and Governance

[ ] Regulatory Compliance: Compliance with relevant laws and regulations (e.g., GDPR, HIPAA).

[ ] Security Policies and Procedures: Documented policies covering cybersecurity best practices.

[ ] Third-Party Audits: Periodic audits to assess security posture.

[ ] Cyber Insurance: Coverage for cybersecurity incidents and data breaches.