SME Cybersecurity & DPDP Compliance Checklist 2025

■ Governance & Compliance

- Appoint a Data Protection Officer (DPO) (if required by DPDP Act).
- Create and publish a data privacy policy for customers.
- Obtain consent management tools for customer data collection.
- Keep records of data processing activities (who collects, who accesses, where it is stored).
- Report data breaches to authorities and affected customers as per DPDP Act timelines.

■ Network Security

- Install firewalls and intrusion detection systems.
- Secure office Wi-Fi with WPA3 encryption.
- Use VPNs for remote employees and hybrid teams.
- Segment networks (e.g., keep IoT devices separate from critical business systems).
- Regularly monitor traffic for suspicious activity.

■ Endpoint Protection

- Deploy endpoint security software on all devices (laptops, desktops, smartphones, tablets).
- Apply automatic OS and software updates.
- Enable full-disk encryption for all company devices.
- Require multi-factor authentication (MFA) for logins.
- Maintain strict device access controls (BYOD policy for employees).

■ Cybersecurity Training & Awareness

- Conduct employee cybersecurity training every 6 months.
- Simulate phishing attacks to test staff awareness.
- Create reporting channels for suspicious emails or behavior.
- Train employees on secure handling of customer data under DPDP.
- Establish a clear IT security policy for staff.

■ Data Breach Prevention & Backup

- Schedule daily automated backups (both local & cloud).

- Store backups in encrypted formats.
- Test recovery plans quarterly.
- Restrict access to sensitive data on a “need-to-know” basis.
- Use data loss prevention (DLP) software to block leaks.

■ Ransomware & Malware Protection

- Install anti-ransomware software.
- Update and patch all systems regularly.
- Disable macros in Microsoft Office documents by default.
- Block suspicious email attachments.
- Maintain an incident response plan in case of attack.

■ Phishing & Social Engineering Protection

- Deploy email filtering solutions.
- Use DKIM, SPF, and DMARC records to secure emails.
- Encourage employees to verify suspicious requests (e.g., payment instructions).
- Establish a report phishing button in email clients.
- Train staff on voice phishing (vishing) awareness.

■ IoT Security

- Change default passwords on all IoT devices.
- Regularly update firmware.
- Isolate IoT devices from the main business network.
- Disable unnecessary features like remote access.
- Monitor IoT traffic for anomalies.

■ Cybersecurity Audits & Assessments

- Conduct an annual cybersecurity audit.
- Perform vulnerability scans quarterly.
- Hire external experts for penetration testing.
- Benchmark against industry frameworks (ISO 27001, NIST, etc.).
- Update security strategy annually.

■ Cyber Insurance & Business Continuity

- Review available cyber insurance policies for SMEs in India.
- Ensure coverage includes ransomware, phishing, and data breaches.
- Document a business continuity plan.
- Run tabletop exercises (mock cyberattack drills).

- Reassess insurance and continuity plans yearly.